ДИПЛОМАТИЧЕСКАЯ АКАДЕМИЯ МИД РОССИИ

III МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ КОНФЕРЕНЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник тезисов

III МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ КОНФЕРЕНЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

III МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ КОНФЕРЕНЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник тезисов

20 ноября 2025 г.

Москва
РИТМ
2026

УДК 004, 327, 339, 341, 342
ББК 3, 65, 66, 67
М43

Рецензенты:
Уланов Александр Андреевич – кандидат экономических наук, проректор по развитию, инновациям и цифровизации Дипломатической академии МИД России;
Смирнов Александр Александрович – доктор юридических наук, доцент, ведущий научный сотрудник 3 отдела НИЦ 4 ВНИИ МВД России

Научный руководитель
Карпович Олег Геннадьевич
заслуженный деятель науки Российской Федерации, доктор юридических наук, доктор политических наук, профессор, и.о. проректора по экспертно-аналитической работе – руководитель Института актуальных международных проблем, заведующий кафедрой стратегических коммуникаций и государственного управления Дипломатической академии МИД России

Ответственные редакторы:
Мартиросян Аревик Жораевна *– кандидат юридических наук, младший научный сотрудник Института актуальных международных проблем, старший преподаватель кафедры государственного управления Дипломатической академии МИД России, член Российской Ассоциации международного права и Молодежного совета Координационного центра доменов.RU/.РФ;*
Себекин Сергей Александрович *– кандидат исторических наук, старший научный сотрудник факультета международных отношений Санкт-Петербургского государственного университета, доцент кафедры политологии, истории и регионоведения Иркутского государственного университета, член исполнительной дирекции Школы МИБ*

М43 III Международная молодежная конференция по информационной безопасности : сборник тезисов / [науч. рук. О.Г. Карпович; отв. ред.: А.Ж. Мартиросян; С.А. Себекин]; Дипломатическая академия МИД России. – Москва: РИТМ, 2026. – 502 с.
ISBN 978-5-98422-807-7.

Сборник тезисов отражает взгляды молодых ученых на проблематику информационно-коммуникационных технологий в контексте развития современных международных отношений, мировой экономики и международного права.

Издание может использоваться в учебном процессе (в учебных организациях высшего образования, где изучают проблемы информационной безопасности), а также учеными, политиками, дипломатами, политологами и другими специалистами в их информационно-аналитической и иной работе.

УДК 004, 327, 339, 341, 342
ББК 3, 65, 66, 67

ISBN 978-5-98422-807-7

СОДЕРЖАНИЕ

ПРОГРАММА III МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10:00-10:30 | **РЕГИСТРАЦИЯ и ПРИВЕТСТВЕННЫЙ КОФЕ**			
10:30 – 11:00 | Ауд.5 | **ОТКРЫТИЕ КОНФЕРЕНЦИИ**			
11:00 – 13:00 **Секция 01** **«Современные вызовы и угрозы информационной безопасности личности и общества»**	11:00 – 14:00 | Ауд.5 **Секция А1** **«Международное управление технологиями ИИ: правовые, политические и этические аспекты глобальной безопасности»**	11:00 – 14:30 | Ауд.27 **Секция В1** **«Национальные и региональные траектории цифрового суверенитета и информационной безопасности»**	11:00 – 12:20 | Онлайн **Секция С1** **«Технологии и кибербезопасность: инфраструктуры, протоколы, угрозы»**
	14:00 – 16:00 | Ауд.5 **Секция А2** **«Цифровая дипломатия, медиа и трансформация международных отношений»**	14:40 – 16:50 | Ауд.27 **Секция В2** **«Технологическая трансформация мировой экономики: искусственный интеллект, отрасли и новые модели управления»**	12:30 – 13:50 | Онлайн **Секция С2** **«Современные цифровые трансформации: от алгоритмов и доверия до интернет-управления»**
	16:00 –18:00 | Ауд.5 **Секция А3** **«Право и безопасность в цифровой среде: ИКТ, искусственный интеллект и нейротехнологии»**	17:00 –18:00 | Ауд.27 **Секция В3** **«Управление интернетом: от нормативно-правовых инструментов до квантовых коммуникаций»**	14:00 –15:30 | Онлайн **Секция С3** **«Цифровые общества и трансформация социально-гуманитарной среды»**
18:00 – 19:30 – фуршет			

ПОРЯДОК РАБОТЫ СЕКЦИЙ

Хаб Самарского национального исследовательского университета им. академика С.П. Королева

11:00 – 13:00

Секция 01
«Современные вызовы и угрозы информационной безопасности личности и общества»

Модератор(ы) секции:

Рощупкин Виталий Геннадьевич – директор Регионального центра развития публичной дипломатии и международных отношений имени Е.М. Примакова (Самарский университет), к.пед.н., доцент.

Докладчики:

1. Горланова М.О. Особенности обеспечения цифрового суверенитета в ведущих странах мира. Самарский национальный исследовательский университет им. академика С.П. Королева.
2. Кривоногов А.А. Проблемы укрепления цифрового суверенитета в России: влияние санкций, киберугроз и импортозамещения. Самарский национальный исследовательский университет им. академика С.П. Королева.
3. Рогов А.С. Современные методы и средства ведения информационно-психологического противоборства (на примере Сирийского конфликта). Самарский национальный исследовательский университет им. академика С.П. Королева.
4. Эргашева С.А. Использование методов информационно-психологического противоборства в ходе арабо-израильского конфликта. Самарский национальный исследовательский университет им. академика С.П. Королева.
5. Исаков Р.О. Инсайдерская информация как угроза информационной безопасности: понятие, информационная и правовая природа. Самарский национальный исследовательский университет им. академика С.П. Королева.
6. Филиппов И.Ю. Проблемы регулирования развития искусственного интеллекта в современном обществе. Самарский национальный исследовательский университет им. академика С.П. Королева.
7. Кох Д.Д. Этические аспекты использования искусственного интеллекта в процессе обучения. Самарский национальный исследовательский университет им. академика С.П. Королева.

8. Муренина А.Г. Особенности правового регулирования создания и распространения электорального контента, сгенерированного искусственным интеллектом. Финансовый университет при Правительстве Российской Федерации.

Аудитория 5

11:00 – 14:00

Секция А1

«Международное управление технологиями искусственного интеллекта: правовые, политические и этические аспекты глобальной безопасности»

Модератор(ы) секции:

Мартиросян Аревик Жораевна – кандидат юридических наук, мл.научный сотрудник Института актуальных международных проблем, доцент кафедры государственного управления Дипломатической академии МИД России, руководитель Школы МИБ, член Молодежного совета Координационного центра доменов.RU/.РФ;

Соловьев Никита Евгеньевич, член Исполнительной дирекции Школы МИБ, член Молодёжного совета Координационного центра доменов .RU/.РФ

Докладчики:

1. Голованова Дарья Александровна. Правовое обеспечение безопасности критической информационной инфраструктуры при внедрении систем искусственного интеллекта. Казанский национальный исследовательский технологический университет (онлайн).
2. Горохова Ульяна Сергеевна. Этика искусственного интеллекта как главный инструмент безопасности в современном информационном мире. Дипломатическая академия МИД России (очно).
3. Зогранян Евгений Владленович. Оправданность использования ИИ в политических целях. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС) (очно).
4. Ивлева Марина Левенбертовна. Цифровизация и проблема трансформации социальной идентичности. РУДН им. Патриса Лумумбы (онлайн).
5. Кадыжев Денис Эльдарович. Искусственный интеллект и трансформация мировой политики и экономики. Дипломатическая академия МИД России (очно).
6. Карасев Павел Александрович. Военно-политические аспекты в контексте глобального регулирования ИИ. ИМЭМО РАН (очно).
7. Малянов Никита Михайлович. Интеграция этических, правовых и технических принципов в развитие искусственного интеллекта. Лениногорский филиал КНИТУ-КАИ (онлайн).
8. Марченко Алина Сергеевна. Искусственный интеллект как инструмент международного контроля: новая архитектура глобального доминирования. МГЛУ (очно).
9. Мацаева Татьяна Владимировна, Макеева Екатерина Антоновна. Укоренение социальной дискриминации в алгоритмах ИИ: анализ расового и гендерного уклона. Иркутский государственный университет (онлайн).
10. Олифиренко Артем Алексеевич. Управление рисками обучения моделей искусственного интеллекта в трансграничной среде. ООО «Экосистема недвижимости

"Метр квадратный"», Саратовская государственная юридическая академия, Саратовский государственный технический университет им. Гагарина Ю.А. (онлайн).

11. Ордин Алексей Вячеславович. Россия и Армения в цифровую эпоху: кибербезопасность и искусственный интеллект как новые измерения международной политики. Министерство промышленности и торговли Российской Федерации, Торгпредство России в Армении (онлайн).

12. Рогожина Евгения Михайловна, Кузнецов Александр Дмитриевич. Реализация инициатив в области международного управления искусственным интеллектом. Нижегородский государственный лингвистический университет им. Н.А. Добролюбова (онлайн).

13. Стрелкова Мария Владимировна. Роль ООН в координации глобальных усилий по регулированию искусственного интеллекта. Российский университет адвокатуры и нотариата имени Г.Б. Мирзоева (очно).

14. Таланкина Любовь Николаевна. Социально-философский анализа влияния ИИ на современные исследования космоса. РУДН им. Патриса Лумумбы (онлайн).

15. Царькова Ольга Олеговна. Позиция Китая в международном регулировании и сотрудничестве в сфере ИИ: влияние на мировой политический ландшафт. НИЯУ МИФИ (очно).

16. Щегрова Алина Николаевна. Институционализация этики: как корпоративное управление делает использование ИИ ответственным. НИЯУ МИФИ (очно).

Аудитория 5

14:00 – 16:00

Секция А2
«Цифровая дипломатия, медиа и трансформация международных отношений»

Модератор(ы) секции:

Мартиросян Аревик Жораевна – кандидат юридических наук, мл.научный сотрудник Института актуальных международных проблем, доцент кафедры государственного управления Дипломатической академии МИД России, руководитель Школы МИБ, член Молодежного совета Координационного центра доменов.RU/.РФ;

Соловьев Никита Евгеньевич, член Исполнительной дирекции Школы МИБ, член Молодёжного совета Координационного центра доменов .RU/.РФ

Докладчики:

1. Мачнев Илья Петрович. Цифровая дипломатия и многосторонние переговоры по Сирии. Новосибирский государственный университет экономики и управления «НИНХ» (онлайн).

2. Тарасенко Ангелина Владимировна. Роль цифровой дипломатии в обеспечении кибербезопасности в XXI веке. Санкт-Петербургский государственный университет (онлайн).

3. Горячева Арина Игоревна. Новые медиа и цифровая дипломатия: трансформация коммуникационных стратегий в современном мире. Новосибирский государственный университет экономики и управления «НИНХ» (очно).

4. Полухина Виктория Дмитриевна. Переосмысление концепции «мягкой силы» в контексте теоретических подходов к международным отношениям XXI века. Новосибирский государственный университет экономики и управления (очно).

5. Сальникова Дарья Анатольевна. На пути к цифровой дисциплине. МГИМО (У) МИД России, ЦИК «Единой России» (очно).

6. Тищенко Владислав Павлович. Создание учебного пособия, направленного на развитие коммуникативных навыков, на основе образовательных журналов. Воронежский государственный педагогический университет (очно).

7. Ямалетдинов Марсель Игоревич. Информационная безопасность и национальная идентичность: символические практики в цифровых медиа российских регионов. ГАУ «Центр гуманитраных исследований Министерства культуры Республики Башкортостан» (онлайн).

8. Матео Рохас Сампер. Магический реализм как механизм эпистемологического сопротивления: переосмысление постколониального суверенитета в условиях ИКТ и глобального управления интернетом. МГИМО (У) МИД России (онлайн).

9. Пикуль Александр Сергеевич. Геометрическое глубокое обучение для детекции дипфейков. Национальный исследовательский университет «Высшая школа экономики» (онлайн).

10. Герасимов Николай Дмитриевич. Визуализация актуальной внешнеполитической проблематики российскими партиями. Мордовский государственный университет имени Н. П. Огарёва (онлайн).

11. Соловьева Александра Ильинична. Цифровая трансформация СМИ в условиях платформенной медиасреды. Дипломатическая академия МИД России (очно).

12. Егорова Екатерина Александровна. Роль американских СМИ как инструмента информационной войны США на территории России (2014-2025). Московский государственный университет им. М.В. Ломоносова (очно).

13. Цао Юнь. Медиа и коммуникация в цифровую эпоху: социально-философский анализ информационной безопасности. РУДН им. Патриса Лумумбы (онлайн).

Аудитория 5

16:00 – 18:00

Секция А3
«Право и безопасность в цифровой среде: ИКТ, искусственный интеллект и нейротехнологии»

Модератор(ы) секции:

Анисимов Игорь Олегович, декан Юридического факультета, кандидат юридических наук, арбитр Арбитражного центра при РСПП, куратор Клуба международного права ДА МИД России;

Мартиросян Аревик Жораевна – кандидат юридических наук, мл.научный сотрудник Института актуальных международных проблем, доцент кафедры государственного управления Дипломатической академии МИД России, руководитель Школы МИБ, член Молодежного совета Координационного центра доменов.RU/.РФ.

Докладчики:

1. Агнистикова Ольга Игоревна. Регулирование ИКТ: противодействие «цифровому колониализму». Казанский (Приволжский) федеральный университет (онлайн).
2. Анисимов Игорь Олегович, Ястребова Алла Юрьевна. Международно-правовая защита персональных данных в современном информационном пространстве. Дипломатическая академия МИД России (очно).
3. Васьков Дмитрий Николаевич, Маслова Елена Михайловна. Институт электронной легализации документов: проблемы и перспективы внедрения в Российской Федерации. Министерство международных и внешнеэкономических связей Свердловской области, МКК, Санкт-Петербургский государственный университет (онлайн).
4. Ветрова Полина Андреевна. Соотношение права на неприкосновенность частной жизни и доступа к персональным данным с целью обеспечения общественной безопасности. Московский государственный юридический университет им. О. Е. Кутафина (онлайн).
5. Гайсин Реналь Радикович. Международное регулирование кибернейробезопасности. Казанский (Приволжский) федеральный университет (онлайн).
6. Глебова Наталья Сергеевна. Борьба с киберпреступностью на примере Организации американских государств. Московский государственный лингвистический университет (очно).
7. Гуляева Елена Евгеньевна. Защита традиционных ценностей в цифровом пространстве Бразилии. Дипломатическая академия МИД России (онлайн).

8. Кортунов Денис Сергеевич. Поддельные нормативные акты как вызов системе политических коммуникаций и национальной безопасности России. Северный (Арктический) федеральный университет им. М.В. Ломоносова (онлайн).

9. Мисаревич Софья Александровна. Правовые риски использования биометрических данных: защита прав граждан и обеспечение безопасности. Казанский национальный исследовательский технологический университет (онлайн).

10. Ниточкин Федор Васильевич. Легитимность власти в условиях цифровизации государственного и муниципального управления. Университет им. О.Е. Кутафина (МГЮА), ФКУ «Аппарат Общественной палаты» (онлайн).

11. Оганесян Тигран Давидович. Современные вызовы защиты данных в условиях развития искусственного интеллекта. Дипломатическая академия МИД России (онлайн).

12. Савельева Наталья Валерьевна. Международно-правовое регулирование центров обработки данных в космосе. ИФЗ РАН, ГЦ РАН (очно).

13. Слесарева Алиса Михайловна. Правовая защита информации в социальных сетях. Казанский национальный исследовательский технологический университет (онлайн).

14. Фролова Валерия Витальевна. Критическая информационная инфраструктура: уязвимости и международная защита. Димитровградский инженерно-технологический институт НИЯУ МИФИ (онлайн).

15. Цыплакова Алёна Дмитриевна. Конвенция ООН против киберпреступности: новшества, перспективы и трудности имплементации для отдельных стран Глобального Юга. МГИМО (У) МИД России (онлайн).

16. Мартиросян А.Ж. Цифровая повестка и ее итоги в 2025: международно-правовая трансформация и геополитические векторы (очно).

Аудитория 27

11:00 – 14:30

Секция B1
«Национальные и региональные траектории цифрового суверенитета и информационной безопасности»

Модератор(ы) секции:

Пичугин Николай Васильевич – мл.н.с., Центр политических исследований и прогнозов, Институт Китая и современной Азии РАН, Член исполнительной дирекции Школы МИБ

Докладчики:

1. Антипов Даниил Романович. Евроатлантическое измерение информационной безопасности Франции. Дипломатическая академия МИД России (очно).

2. Архипенко Серафим Юрьевич. Цифровой суверенитет как основа национальной и международной информационной безопасности. Белорусский государственный университет (онлайн).

3. Бобер Александр Евгеньевич. Национальная информационная сеть Ирана: цифровой суверенитет как инструмент внешней политики. Сибирский институт управления - филиал РАНХиГС (онлайн).

4. Бутенко Сергей Викторович. Понятие идентичности в эпоху цифровой трансформации российского общества. РУДН им. Патриса Лумумбы (онлайн).

5. Головач Павел Николаевич. Стратегические основы обеспечения информационной безопасности и цифрового суверенитета в рамках Организации договора о коллективной безопасности: современные угрозы и перспективы совершенствования. Белорусский государственный университет (онлайн).

6. Гришанина Татьяна Александровна. Цифровая стратегия Израиля в условиях неопределённости на Ближнем Востоке. Независимый исследователь (онлайн).

7. Джавад Ольга Васильевна. Культура национальной безопасности как феномен эпохи цифровизации российского общества. РУДН им. Патриса Лумумбы (онлайн).

8. Джуматаева Юлия Искандеровна. Цифровой суверенитет и национальные стратегии обеспечения информационной безопасности. Дипломатическая академия МИД России (очно).

9. Иванов Евгений Олегович. Сотрудничество государств Латинской Америки по обеспечению безопасности ИКТ в рамках ОАГ. МГИМО (У) МИД России (очно).

10. Мамедзада Камандар Захид оглы. Роль Государственной службы специальной связи и информационной безопасности Азербайджана в обеспечении информационной безопасности. РУДН (очно).

11. Мирзоев Эмин Эльчинович. Информационное противостояние в АТР: политические технологии как инструменты формирования новой реальности. Тюменский государственный университет (онлайн).

12. Ордин Алексей Вячеславович. Новые рубежи международной сертификации и доверия в кибербезопасности: опыт CREST и перспективы применения NGFW-технологий в рамках цифрового суверенитета. Министерство промышленности и торговли Российской Федерации, Торгпредство России в Армении (онлайн).

13. Пичугин Николай Васильевич. Сервисная система жалоб населения - основа для саморегулирования информационного пространства КНР. Института Китая и современной Азии РАН, Исполнительная дирекция Школы МИБ (очно).

14. Попович Иван Владимирович. Кризис международной информационной безопасности в Балтийском регионе. Дипломатическая академия МИД России (очно).

15. Пьянникова Дарья Евгеньевна. Информационная интеграция государств-членов ЕАЭС в рамках формирования единого цифрового пространства. Уральский федеральный университет (онлайн).

16. Ракова Екатерина Дмитриевна. Стратегическое партнёрство России и Ирана в киберпространстве противодействие глобальным угрозам и перспективы всеобъемлющего сотрудничества. Международная академия бизнеса и управления (очно).

17. Сакович Анастасия Дмитриевна. Цифровая безопасность на Курильских островах: вызовы и перспективы в условиях современных угроз. Казанский (Приволжский) федеральный университет (онлайн).

18. Суховерхова Анастасия Игоревна. Особенности системы обеспечения информационной безопасности в Германии. Дипломатическая академия МИД России (очно).

19. Яникеева Инна Олеговна. Конструирование киберугроз в дискурсе США: кейс администрация Дж. Байдена. Национальный исследовательский университет «Высшая школа экономики» (онлайн).

20. Шемякина Яна Валерьевна. Международная информационная безопасность: тенденции и перспективы. Независимый исследователь (онлайн).

Аудитория 27

14:40 – 16:50

Секция В2
«Технологическая трансформация мировой экономики: искусственный интеллект, отрасли и новые модели управления»

Модератор(ы) секции:

Пичугин Николай Васильевич – мл.н.с., Центр политических исследований и прогнозов, Институт Китая и современной Азии РАН, Член исполнительной дирекции Школы МИБ

Докладчики:

1. Вагнер Александр. Применение ИИ в противодействии отмыванию денег и мошенничеству: эффективность, соответствие регуляторным требованиям и объяснимость моделей. Финансовый университет при Правительстве Российской Федерации (онлайн).

2. Внучкова Ульяна Андреевна, Казаченков Станислав Дмитриевич, Карапетян Марина Седраковна. Этико-правовые вызовы и регуляторные перспективы внедрения искусственного интеллекта в финансово-правовую сферу России. Ростовский государственный экономический университет (РИНХ) (онлайн).

3. Махнев Никита Дмитриевич, Пароваткина Дарья Ивановна. Геосервисы как инструмент разработки и продвижения брендингового туристического маршрута (на примере «Катунской тропы» в Алтайском крае). Алтайский государственный университет, Бийский филиал (онлайн).

4. Плехова Ирина Андреевна, Чашкина Любовь Владимировна. Искусственный интеллект и будущее профессий: влияние технологий искусственного интеллекта на рынок труда и потребности в компетенциях сотрудников. Шадринский финансово-экономический колледж филиал Федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации» (онлайн).

5. Поникаровских Полина Павловна, Оболдина Ангелина Викторовна. Искусственный интеллект и трансформация мировой политики и экономики. Шадринский финансово-экономический колледж филиал Федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации» (онлайн).

6. Салахова Камила Анфасовна. Цифровая гегемония как форма неоколониализма: право на киберсуверенитет в XXI веке. Дипломатическая академия МИД России (очно).

7. Сюй Жуйлинь. Вызовы для российско-китайского сотрудничества в сфере цифровой экономики. РУДН им.Патриса Лумумбы (онлайн).

8. Уфимцев Андрей Владимирович. Экономико-управленческие аспекты внедрения систем усовершенствованного управления на основе математического моделирования в нефтегазовой отрасли. Томский политехнический университет (очно).

9. Федоров Евгений Михайлович. Влияние информационных технологий на логистическую отрасль. ЗАО «Промтрактор – Вагон» (очно).

10. Цзинсюй У. Минимально достаточная архитектура управления киберрисками АЭС в условиях цифрового суверенитета России. Московский государственный университет им. М.В. Ломоносова (очно).

11. Чебакова Варвара Михайловна. Киберустойчивость промышленных предприятий – стратегический актив. Омский государственный технический университет (онлайн).

12. Чернобривченко Анастасия Олеговна. Роль цифровой трансформации в развитии нефтегазовой отрасли на примере компании British Petroleum. РГУ Нефти и газа им. И.М. Губкина (онлайн).

13. Чубаров Николай Александрович. Цифровое неравенство в управлении данными. РУДН им. Патриса Лумумбы (онлайн).

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ

17:00 – 18:00

Секция В3
«Управление интернетом: от нормативно-правовых инструментов до квантовых коммуникаций»

организована совместно с Молодежным советом Координационного центра доменов .RU/.РФ

Модератор(ы) секции:

Алейников Андрей Алексеевич, руководитель группы по связям с общественностью, председатель Молодежного совета Координационного центра доменов .RU/.РФ.

Докладчики:

1. Бородина Полина Сергеевна. Квантовые коммуникации как стратегический приоритет в обеспечении цифрового суверенитета России. Московский технический университет связи и информатики, Школа МИБ, Молодёжный совет Координационного центра доменов .RU/.РФ (очно).

2. Геращенко Алёна Игоревна. Правовые и организационные вопросы идентификации пользователей сети Интернет: российский и зарубежный опыт [1]. Национальный исследовательский университет «Высшая школа экономики», Молодёжный совет Координационного центра доменов .RU/.РФ (онлайн).

3. Игнатов Александр Александрович. Позиции стран БРИКС на переговорах по международной информационной безопасности в рамках ООН. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС), Молодёжный совет Координационного центра доменов .RU/.РФ (онлайн).

4. Савельева Анастасия Андреева. Обзор подходов и стандартов к распределенному мультизональному хранению и обработке данных. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Молодёжный совет Координационного центра доменов .RU/.РФ (онлайн).

5. Свиридова Алина Игоревна. Искусственный интеллект как фактор изменения баланса сил: гонка технологических экосистем. Национальный исследовательский университет «Высшая школа экономики», Молодёжный совет Координационного центра доменов .RU/.РФ (онлайн).

[1] Исследование выполнено за счет гранта Российского научного фонда (проект № № 25-18-00698 «Организационно-правовые аспекты устойчивого и бережного оборота данных в условиях цифровой трансформации» https://rscf.ru/project/25-18-00698/).

6. Соловьев Никита Евгеньевич. Институциональная инерция разработчиков как фактор усиления уязвимостей генеративного искусственного интеллекта. Исполнительная дирекция Школы МИБ, Молодёжный совет Координационного центра доменов .RU/.РФ (очно).

7. Тюлякова Софья Андреевна. Построение семантических деревьев нормативно-правовых актов как инструмент эффективного государственного управления. МГЛУ, Молодёжный совет Координационного центра доменов .RU/.РФ (очно).

8. Тюмин Сергей Григорьевич. DDoS-атаки на российские доменные зоны: угрозы и методы противодействия. МТУСИ, Молодёжный совет Координационного центра доменов .RU/.РФ (очно).

Онлайн
Хаб Иркутского государственного университета

11:00 – 12:20

Секция С1
«Технологии и кибербезопасность: инфраструктуры, протоколы, угрозы»

Модератор(ы) секции:

Себекин Сергей Александрович – к.и.н., старший научный сотрудник факультета международных отношений СПбГУ, доцент кафедры политологии, истории и регионоведения Иркутского государственного университета, член Исполнительной дирекции Школы МИБ.

Докладчики:

1. Болданова Дарья Булатовна. Либеральная конструкция нелиберального мира: как цепочки поставок шпионского программного обеспечения способствуют авторитарному управлению конфликтами. Школа МИБ (онлайн).

2. Багрова Анна Владимировна, Цабей Анна Алексеевна. Киберугрозы системе □C□RS: анализ уязвимостей и пути повышения безопасности авиационной связи. Новосибирский государственный технический университет НЭТИ (онлайн).

3. Папе Алексей Владиславович. Kerberos: особенности генерации и использования файла ключей в мультиОС-инфраструктуре. Поволжский государственный университет телекоммуникаций и информатики (очно).

4. Чжан Цзинхуэй. От 5G к межграничным волоконно-оптическим линиям: стратегическая практика совместного строительства «цифровой артерии». Казахский Национальный Университет имени Аль-Фараби (онлайн).

5. Рагозин Валентин Никитич. Польза open-source технологий в государственном ИТ-секторе и вред для коммерческого сектора. Независимый исследователь (онлайн).

6. Морозова Полина Евгеьевна. Разработка системы биометрической аутентификации на основе ЭКГ. Национальный исследовательский университет ИТМО (онлайн).

Онлайн

Хаб РУДН им. Патриса Лумумбы и Иркутского государственного университета

12:30 – 13:50

Секция С2
«Современные цифровые трансформации: от алгоритмов и доверия до интернет-управления»

Модератор(ы) секции:

Себекин Сергей Александрович – к.и.н., старший научный сотрудник факультета международных отношений СПбГУ, доцент кафедры политологии, истории и регионоведения Иркутского государственного университета, член Исполнительной дирекции Школы МИБ.

Джавад Ольга Васильевна – старший преподаватель кафедры социальной и политической философии РУДН им. Патриса Лумумбы.

Докладчики:

1. Чекулаев Василий Олегович. Киберпсихология и формирование общественного мнения в условиях цифровых технологий. Иркутский государственный университет (онлайн).
2. Лиман Полина Сергеевна. Доверие как ресурс цифрового суверенитета: восприятие национального мессенджера «М□Х» в российском обществе. Санкт-Петербургский государственный университет (онлайн).
3. Иванова Ксения Олеговна, Дуев Илья Витальевич. Факторы, влияющие на готовность людей мириться с нарушением конфиденциальности их личной информации со стороны государства. Национальный исследовательский университет «Высшая школа экономики» (онлайн).
4. Чуклина Элена Юрьевна. Ограничения и запреты потребления контента в сети «Интернет». ЮНЦ РАН (онлайн).
5. Денисенко Светлана Ильинична, Кропачев Святослав Сергеевич. Цифровой суверенитет: перспективы «(де)централизации» в современном мире. Национальный исследовательский университет «Высшая школа экономики» – Санкт-Петербург (онлайн).
6. Муравьева Полина Владимировна. Международное управление интернетом и цифровая архитектура будущего. Санкт-Петербургский государственный университет (онлайн).
7. Фомина Софья Ивановна. Влияние алгоритмов на политические предпочтения. Иркутский государственный университет (онлайн).

Онлайн

Хаб Иркутского государственного университета

14:00 – 15:30

Секция С3
«Цифровые общества и трансформация социально-гуманитарной среды»

Модератор(ы) секции:

Себекин Сергей Александрович – к.и.н., старший научный сотрудник факультета международных отношений СПбГУ, доцент кафедры политологии, истории и регионоведения Иркутского государственного университета, член Исполнительной дирекции Школы МИБ.

Докладчики:

1. Санникова Елизавета Сергеевна. Социальные последствия внедрения метавселенных. Иркутский государственный университет (онлайн).
2. Матвейчук Захар Евгеньевич. ИИ как инструмент региональной безопасности в рамках ШОС: кейс наркотрафика в «Золотом треугольнике» Иркутский государственный университет (онлайн).
3. Стасяк Павел Валентинович. Экономика сновидений: может ли ИИ управлять ресурсами в метавселенных? Белорусский государственный музей народной архитектуры и быта (онлайн).
4. Масленников Александр Эдуардович. Рекомендательная система культурных событий: гибридные алгоритмы для ценностно-ориентированного выбор. Южный университет (ИУБиП) (онлайн).
5. Водопьянова Мария Константиновна, Дрюпина Владислава Борисовна. Информационная безопасность музеев: от уязвимостей к системной защите культурного наследия. Уральский государственный юридический университет им. В. Ф. Яковлева (онлайн).
6. Карапетова Розалина Валерьевна. Сохранение исторической памяти о геноциде советского народа нацистами и их пособниками в годы Великой Отечественной Войны на оккупированной территории «нюрнбергский процесс: без срока давности» на основе возможностей искусственного интеллекта. ГБПОУ Краснодарского края «Краснодарский педагогический колледж» (онлайн).
7. Абдулаев Роберт Альбертович. Использование цифровых образовательных ресурсов в системе СПО на занятиях по дисциплине «Информатика» сегодня. Государственное автономное профессиональное образовательное учреждение Самарской области «Самарский колледж сервиса производственного оборудования им. Героя Российской Федерации Е.В. Золотухина» (онлайн).
8. Черненко Алина Сергеевна. Использование нейросетей на уроке литературного чтения в начальных классах. ГБПОУ Краснодарского края «Краснодарский педагогический колледж» (онлайн).

9. Волченкова Александра Викторовна. Кибербезопасность современного школьника. Как не стать жертвой интернет-мошенничества. РУДН им. Патриса Лумумбы (онлайн).

10. Прокопчук Дарья Эдуардовна. Мониторинг цифрового сознания студентов с использованием интеллектуального анализа. Южный университет (ИУБиП) (онлайн).

11. Себекин Сергей Александрович. Стратегическая коммуникация БРИКС в эпоху искусственного интеллекта и инфократии: как инклюзивная коммуникация заменяется синтетическим информационным потоком Иркутский государственный университет, Исполнительная дирекция Школы МИБ.

ТЕЗИСЫ ДОКЛАДОВ УЧАСТНИКОВ

III МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Секция 01 «Современные вызовы и угрозы информационной безопасности личности и общества»

Мария Олеговна Горланова,
ассистент кафедры безопасности информационных систем
Самарский национально исследовательский университет,
E-mail: gm763@yandex.ru

Mariia O. Gorlanova,
Associate Professor, Department of Information Systems Security ,
Samara National Research University,
E-mail: gm763@yandex.ru

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА В ЕС, США, КИТАЕ

SPECIFICITIES OF ENSURING DIGITAL SOVEREIGNTY IN THE EU, US, AND CHINA

Аннотация. В статье сравниваются подходы к цифровому суверенитету в ЕС, США и Китае на основе анализа ключевых стратегических документов. Показано, что ЕС делает акцент на защите прав граждан и снижении внешней технологической зависимости, США – на поддержании глобального технологического лидерства, а Китай – на укреплении государственного контроля и политической стабильности. Сравнение демонстрирует, что цифровой суверенитет становится важным инструментом национальной безопасности и геополитической конкуренции.

Ключевые слова: цифровой суверенитет, национальная безопасность, кибербезопасность, стратегические документы, ЕС, США, Китай.

Abstract. This paper compares the approaches to digital sovereignty in the EU, the United States, and China based on an analysis of key strategic documents. The study shows that the EU prioritizes the protection of citizens' rights and the reduction of technological dependence, the US focuses on maintaining global technological leadership, and China emphasizes state control and political stability. The comparison demonstrates that digital sovereignty has become a central instrument of national security and geopolitical competition.

Key words: digital sovereignty, national security, cybersecurity, strategic documents, EU, USA, China.

Определение понятия цифровой суверенитет. Современное технологическое развитие существенно изменило не только повседневную жизнь, но и политическую сферу. Ведущие страны мира всё чаще поднимают вопрос цифрового суверенитета – необходимости контроля и защиты цифрового пространства на национальном уровне. Цель данного исследования – выявить особенности реализации цифрового суверенитета в странах ЕС, США, Китае. В научной литературе и международной практике нет единого определения цифрового суверенитета, что

связано с различиями в политических и культурных приоритетах стран. Рассматривая существующие концепции данного понятия [1], можно классифицировать подходы как государственный цифровой суверенитет и народный цифровой суверенитет. Народный цифровой суверенитет подразумевает основным носителем суверенитета в киберпространстве должны стать люди, которые пользуются интернетом, а не национальные государства, данный подход фокусируется на сохранение первоначальной концепции интернета, в которой отсутствует государственный контроль.

Государственный цифровой суверенитет определятся каждой страной по-разному с учетом политических и культурных особенностей. Страны ЕС цифровой суверенитет рассматривают через призму защиты персональных данных, стратегической цифровой инфраструктуры и соблюдения европейских ценностей [2]. Ляо Фань в своем исследовании [3] пишет о том, что Китай определяет цифровой суверенитет как естественное продолжение национального суверенитета в цифровой сфере, которое проявляется как высшая внутренняя юрисдикция государства и внешняя независимость в цифровой сфере, как и традиционный суверенитет [3]. С. Кутюр С. Тоупин в совместной работе [1] пишут о том, что в США цифровой суверенитет имеет негативную коннотацию, вместо этого они используют понятие технологического лидерства, которое подразумевает глобальное доминирование в критических и новых технологиях (ИИ, квантовые технологии, биотехнологии, полупроводники), поддержку промышленной базы, стандартизацию и коммерциализацию инноваций [4].

Национальные подходы к цифровому суверенитету через стратегии. Для анализа национальных подходов к цифровому суверенитету выбраны ключевые стратегические документы, определяющие цели, принципы и приоритетные направления развития цифровой сферы.

Европейский союз в стратегическом документе по цифровому развитию [5] декларируется европейский путь к цифровизированной экономике и обществу основан на солидарности, процветании и устойчивом развитии, укорененном в расширении прав и возможностей граждан и предприятий, обеспечении безопасности и устойчивости цифровой экосистемы. Так же в данном документе фиксируется угроза высокой технологической зависимости от внешних стран. Для дальнейшего цифрового развития ЕС ставит следующие цели:

- повышение цифровой грамотности среди населения и привлечение высококвалифицированных ИТ-специалистов;
- обеспечение цифровой инфраструктуры;
- цифровая трансформация бизнеса;
- цифровизация государственных услуг.

Таким образом страны ЕС в первую очередь связывают развитие цифрового пространства с защитой прав человека демократических институтов, устойчивостью цифровой экономики и уменьшением зависимости от внешних поставщиков критических технологий.

В Национальной стратегии кибербезопасности США цифровая сфера рассматривается прежде всего через призму угроз внешнего воздействия. К числу ключевых угроз относят кибершпионаж, кражу интеллектуальной собственности, распространение вредоносного программного обеспечения, деятельность преступных группировок и государств-противников, включая Китай и Россию.

Стратегия строится на пяти опорных направлениях:

1.Защита критической инфраструктуры с акцентом на повышение устойчивости цифровых систем и ответственности операторов инфраструктуры за безопасность.

2. Выявление и нейтрализация акторов угроз, включая совместные действия государства, разведки, частного сектора и международных партнеров.

3. Формирование рыночных стимулов безопасности, что предполагает возложение ответственности на разработчиков небезопасного ПО, усиление регулирования качества кибербезопасности и поддержку инновационных архитектур безопасности.

4. Инвестирование в безопасные технологии будущего, включая поддержку исследовательских центров, промышленной базы и разработку стандартов.

5. Создание сети международных союзников для совместного противоействия киберугрозам, укрепления норм поведения в цифровой среде и обеспечения стабильности глобальных цепочек поставок [6].

Таким образом, подход США к цифровому суверенитету носит технологический и стратегический характер.

Национальная стратегия кибербезопасности Китая определяет широкий спектр угроз, среди которых числится вмешательство иностранных государств во внутренние дела, подрыв политической стабильности, распространение сепаратистских и экстремистских материалов, утрата культурных ценностей, кибератаки на экономику и критическую инфраструктуру. В отличие от США, акцентирующих внимание на технологических угрозах и кибершпионаже, Китай выделяет прежде всего политико-идеологические и социальные угрозы, что отражает особенности его модели государственного управления. Документ формулирует восемь ключевых задач:

1. Защита государственного суверенитета в цифровой сфере, что включает полный контроль над цифровой инфраструктурой, интернет-платформами и трансграничными потоками данных.

2. Обеспечение национальной безопасности, противодействие подрывной деятельности, иностранному вмешательству, утечкам секретной информации.

3. Защита критической информационной инфраструктуры через мониторинг, раннее предупреждение, обязательные меры безопасности и централизованный контроль.

4. Формирование позитивной онлайн-культуры, продвижение национальных ценностей, борьба с «вредным контентом» и защита несовершеннолетних.

5. Борьба с кибертерроризмом и преступностью, включая кибершпионаж, мошенничество, незаконный оборот данных и хакерские атаки.

6.Совершенствование системы управления интернетом, развитие нормативной базы, создание отраслевых стандартов и укрепление индустрии кибербезопасности.

7. Повышение кибероборонь, развитие технологий для отражения атак и защиты стратегических систем.

8. Международное сотрудничество, направленное на формирование альтернативной глобальной модели интернет-управления и сокращение цифрового неравенства для развивающихся стран [7].

Подход Китая к цифровому суверенитету основан на расширенной трактовке государственного контроля и приоритете политической стабильности. Если ЕС делает акцент на правах человека и технологической автономии, а США – на глобальном технологическом лидерстве, то Китай рассматривает цифровой суверенитет как инструмент защиты национального суверенитета, идеологии и социального порядка, стремясь формировать собственную модель глобального цифрового управления.

Заключение. Анализ стратегических документов ЕС, США и Китая показывает, что, несмотря на различия в политических моделях, ценностях и подходах к регулированию цифровой сферы, все эти государства признают цифровой суверенитет важнейшим элементом национальной безопасности и глобального позиционирования. Однако содержание понятия «цифровой суверенитет» существенно различается в зависимости от национальных приоритетов. Для ЕС оно связано прежде всего с защитой прав граждан, обеспечением устойчивости цифровой инфраструктуры и снижением стратегической зависимости от внешних поставщиков технологий. США, напротив, рассматривают цифровую сферу через призму технологического лидерства, стремясь удерживать глобальное доминирование в критических технологиях и укреплять позиции в международной стандартизации. Китай же трактует цифровой суверенитет как расширение традиционного государственного суверенитета, акцентируя внимание на политической стабильности, контроле над данными и информационными потоками и защите национальной идеологии. Несмотря на эти различия, общим для всех стран является стремление

укреплять контроль над цифровой инфраструктурой, развивать собственные технологические экосистемы и повышать устойчивость к киберугрозам. Цифровой суверенитет становится универсальным инструментом реализации политических и экономических интересов государств, отражая более широкий тренд на фрагментацию глобального цифрового пространства. В условиях растущей конкуренции ведущие мировые игроки стремятся не только защитить свои внутренние цифровые системы, но и сформировать выгодные для себя модели международного цифрового порядка. Это свидетельствует о том, что цифровой суверенитет из узкой технической категории превращается в ключевую составляющую глобальной геополитики и стратегического развития.

Список источников и литературы:

1. С. Кутюр, С. Тоупин. Что означает понятие «суверенитет» в цифровом мире? – 2020 [Электронный ресурс] // Вестник международных организаций. URL: https://iorj.hse.ru/2020-15-4/416597980.html (дата обращения: 25.10.2025).

2. Digital sovereignty and autonomy [Электронный ресурс] // interoperble europe URL: https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap/digital-sovereignty-and-autonomy (дата обращения: 25.10.2025).

3. 廖凡 数字主权与全球数字治理 [Электронный ресурс] // School of law, University of Chinese Academy of Social Sciences. URL: https://law.ucass.edu.cn/info/1985/7542.htm (дата обращения: 27.10.2025).

4. NIST Strategy for American Technology Leadership in the 21st Century [Электронный ресурс] // National Institute of Standards and Technology. URL: https://www.nist.gov/director/strategic-priorities (дата обращения: 1.11.2025).

5. 2030 Digital Compass: the European way for the Digital Decade [Электронный ресурс] // EUROPEAN COMMISSION. URL: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf (дата обращения: 1.11.2024).

6. National Cybersecurity Strategy 2023 [Электронный ресурс] // BIDENWHITEHOUSE URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения: 3.11.2025).

7. National Cyberspace Security Strategy [Электронный ресурс] // China Copyright and Media The law and policy of media in China – edited by Rogier Creemers. URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (дата обращения: 5.11.2024).

Антон Александрович Кривоногов,
Студент группы 4443-100301D, кафедры безопасности информационных систем,
Механико-математический факультет
Самарский национальный исследовательский университет имени С.П.Королева,
E-mail: antonkrivonogov081004@yandex.ru

Anton A. Krivonogov,
Student, Group 4443-100301D, Department of Information Systems Security,
Faculty of Mechanics and Mathematics
Samara National Research University named after S.P. Korolev,
Email: antonkrivonogov081004@yandex.ru

ПРОБЛЕМЫ УКРЕПЛЕНИЯ ЦИФРОВОГО СУВЕРЕНИТЕТА В РОССИИ: ВЛИЯНИЕ САНКЦИЙ, КИБЕРУГРОЗ И ИМПОРТОЗАМЕЩЕНИЯ

CHALLENGES OF STRENGTHENING DIGITAL SOVEREIGNTY IN RUSSIA: THE IMPACT OF SANCTIONS, CYBER THREATS AND IMPORT SUBSTITUTION

Аннотация. Автором раскрыты ключевые проблемы укрепления цифрового суверенитета России в условиях западных санкций, растущих киберугроз и сложностей импортозамещения. Рассмотрены положения Федерального закона № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», противосанкционного законодательства и их практическая реализация. Проанализированы данные о сокращении российских серверов, росте кибератак на 65% в 2025 году, достижении 15-20% импортозамещения в ИТ секторе.

Ключевые слова: цифровой суверенитет, санкции, киберугрозы, импортозамещение, критическая информационная инфраструктура, суверенный интернет, Россия.

Abstract. The author explores the key challenges of strengthening Russia's digital sovereignty in the face of Western sanctions, growing cyber threats, and the challenges of import substitution. The article examines the provisions of Federal Law No. 187-FZ of July 26, 2017, «On the Security of the Critical Information Infrastructure of the Russian Federation», anti-sanctions legislation, and their practical implementation. It also analyzes data on the decline of Russian servers, a 65% increase in cyberattacks by 2025, and the achievement of 15-20% import substitution in the IT sector.

Key words: digital sovereignty, sanctions, cyber threats, import substitution, critical information infrastructure, sovereign internet, Russia.

Законодательные основы цифрового суверенитета. Укрепление цифрового суверенитета России представляет собой стратегическую задачу, закрепленную в Федеральном законе № 149-

ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. [11]. Данный закон предусматривает установку оборудования для противодействия угрозам и централизованное управление сетями, создавая правовую базу для автономного функционирования Рунета.

Критическая информационная инфраструктура (КИИ) регулируется Федеральным законом № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации», с поправками от Федерального закона № 58-ФЗ от 7 апреля 2025 г., обязывающими субъекты КИИ использовать российское программное обеспечение [7,8]. Защита персональных данных обеспечивается Федеральным законом № 152-ФЗ от 27 июля 2006 г., требующим локализации данных на территории России [9].

Программа «Цифровая экономика Российской Федерации», утвержденная Постановлением Правительства РФ № 1632-р от 28 декабря 2017 г. и продленная до 2030 года, направлена на комплексное развитие цифровой инфраструктуры и технологической независимости [5].

Киберугрозы как фактор риска. Рост кибератак на российскую инфраструктуру в 2025 году достиг 65% по сравнению с предыдущим годом, с фокусом на финансовый сектор, государственные органы и критическую инфраструктуру. Основные типы киберугроз включают Denial of Service (DDoS) атаки, вредоносное программное обеспечение (ПО) (malware, ransomware), фишинг и атаки на цепочки поставок через компрометацию программного обеспечения.

Проблемы импортозамещения в ИТ-секторе. Программа импортозамещения, основанная на Федеральном законе № 488-ФЗ от 31 декабря 2014 г. «О промышленной политике в Российской Федерации» и Указе Президента РФ № 166 от 30 марта 2022 г., показала неоднозначные результаты [6,10]. К 2021 году в государственных компаниях был достигнут уровень замещения в 30-35%, а к началу 2025 года только 15-20% компаний в целом перешли на российские решения [1]. Наблюдается дифференциация по секторам: в публичном секторе импортозамещение достигло 43%, тогда как в частном бизнесе показатели ниже 10-15%. Основные причины низкой эффективности включают высокие цены на российское ПО при низком качестве, проблемы несовместимости, дефицит квалифицированных специалистов и недостаточное финансирование исследований и разработки (R&D). В кибербезопасности замещение достигло 90-100% для ПО согласно требованиям Федерального закона № 187-ФЗ с поправками № 58-ФЗ, но аппаратные компоненты остаются уязвимыми [7,8]. Отказ от создания полностью отечественной ИТ-экосистемы привел к стратегии замены западных поставщиков на китайских, что не решает проблему технологической зависимости. Программа «Цифровая

экономика» предусматривает достижение 95% отечественного ПО в ключевых отраслях к 2030 году, но этот показатель выглядит нереалистичным при текущих темпах прогресса [4].

Оценка достижений и перспективы. По заявлению первого заместителя руководителя администрации президента РФ Сергея Кириенко на РИФ-2025, Россия вошла в число трех стран мира, обладающих полной экосистемой цифрового суверенитета наряду с США и Китаем [3]. Экономика российского сегмента интернета второй год растет более чем на 40%, а наличие мощных национальных платформ и зрелой экосистемы цифровых услуг, подкрепленные государственной поддержкой, позволили минимизировать негативное воздействие санкций [2]. Российская интернет-экономика эффективно адаптируется к изменяющимся реалиям, отечественные сервисы завоевывают лояльность аудитории. Однако остаются серьезные проблемы: дефицит специалистов, ограниченный доступ к передовым технологиям, риски технологического отставания и зависимость от китайских поставщиков.

Заключение. Укрепление цифрового суверенитета России осложняется рядом взаимосвязанных факторов, для преодоления которых необходимы комплексные меры: увеличение инвестиций в отечественные разработки, развитие международного сотрудничества в рамках БРИКС и ШОС, совершенствование законодательства, создание условий для возвращения ИТ-специалистов, а также баланс между безопасностью и открытостью для предотвращения полной изоляции от глобальной цифровой экосистемы. Планируемое достижение 95% отечественного ПО в ключевых отраслях к 2030 году требует решения текущих проблем качества, совместимости и дефицита специалистов, чтобы закрепить основы долгосрочной технологической независимости России.

Список источников и литературы:

1. Импортозамещение? Только 35% компаний реально перешли на российское ПО [Электронный ресурс] // Securitylab. URL: https://clck.ru/3QGSa3 (дата обращения: 10.11.2025).
2. Кириенко заявил об информационном давлении на российскую интернет-отрасль [Электронный ресурс] // РИА Новости. URL: https://clck.ru/3QGSfU (дата обращения: 10.11.2025).
3. Кириенко: Россия вошла в тройку стран с полным цифровым суверенитетом [Электронный ресурс] // Ведомости. URL: https://clck.ru/3QGSdJ (дата обращения: 10.11.2025).
4. Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс] // Минцифры. URL: https://clck.ru/3QGSbW (дата обращения: 10.11.2025).
5. Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGSSz (дата обращения: 10.11.2025).

6. Указ Президента РФ от 30.03.2022 N 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGSYB (дата обращения: 10.11.2025).
7. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ» [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGS2R (дата обращения: 10.11.2025).
8. Федеральный закон от 07.04.2025 N 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGS3t (дата обращения: 10.11.2025).
9. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGSJE (дата обращения: 10.11.2025).
10. Федеральный закон «О промышленной политике в Российской Федерации» от 31.12.2014 N 488-ФЗ [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGSWw (дата обращения: 10.11.2025).
11. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QGRuQ (дата обращения: 10.11.2025).

Самира Аббасовна Эргашева,
студентка III курса исторического факультета направления подготовки «Международные отношения и внешняя политика»
гр. 5302-410305D,
Самарский университет,
E-mail: samiraergasheva8@gmail.com

Samira Ab. Ergasheva,
3-rd year student of Faculty of History, field of study International Relations and Foreign Policy,
5302-410305D,
Samara University,
E-mail: samiraergasheva8@gmail.com

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ПРОТИВОБОРСТВА В ХОДЕ АРАБО-ИЗРАИЛЬСКОГО КОНФЛИКТА

USE OF INFORMATION AND PSYCHOLOGICAL CONFRONTATION METHODS DURING THE ARAB-ISRAELI CONFLICT

Аннотация. В данной работе на основе сравнительного анализа статей от международной телекомпании AlJazeera (Катар) и еврейской международной правозащитной организации American Jewish Committee (США) рассматривается освещение в СМИ истоков и причин арабо-израильского конфликта на фоне нового витка эскалации палестино-израильского конфликта после событий 7 октября 2023 года. В результате были выявлены основные методы, способы и приемы, к которым прибегают авторы статей при изложении фактов для формирования у читателей и аудитории наиболее выгодной и желанной позиции относительно ситуации на Ближнем Востоке. Таким образом, в данной работе СМИ, в первую очередь, выступают, как площадка для трансляции нарративов и пропаганды.

Ключевые слова: AlJazeera, American Jewish Committee, Палестина, Израиль, СМИ, арабо-израильский конфликт.

Abstract. This work, based on a comparative analysis of articles from the international television company AlJazeera (Qatar) and the Jewish international human rights organization American Jewish Committee (USA), examines the media coverage of the origins and causes of the Arab-Israeli conflict in the context of the new escalation of the Palestinian-Israeli conflict following the events of October 7, 2023. As a result, the main methods, ways, and techniques used by the authors of the articles to present facts in order to shape the most favorable and desirable position for readers and audiences regarding the situation in the Middle East have been identified. Thus, in this work, the media primarily acts as a platform for broadcasting narratives and propaganda.

Key words: AlJazeera, American Jewish Committee, Palestine, Israel, the media, Arab-Israeli conflict.

Развитие цифровых технологий вывело на новый уровень информационные войны, где участниками чаще всего теперь выступают электронные СМИ. Именно цифровые медиа начинают все более активную роль играть в информировании, образовании и социализации граждан, а также в формировании общественного мнения. Многим современным медиа при освещении эскалаций международных конфликтов свойственно обращаться к их истокам и разъяснять события прошлого, для того, чтоб показать читателю причинно-следственную связь. Но, с учетом ангажированности СМИ, нетрудно предположить, что каждое агентство может трактовать исторические факты в своих интересах, тем самым создавая более выгодное положение для одной из сторон противостояния.

Обострение ситуации на Ближнем Востоке в октябре 2023 года не только в очередной раз поставило палестино-израильский конфликт в центр международной повестки, но и буквально раскололо мировое сообщество, представители которого оказались по разную сторону баррикад. Именно поэтому рассмотреть способы противоборства в СМИ мы попробуем на примере палестино-израильского конфликта, вокруг которого разразилась самая настоящая информационная война, подогреваемая мировыми медиа.

Цель данного исследования – на основе сравнения СМИ выявить широко используемые ими методы в ходе информационного противостояния вокруг дискуссий об истоках и причинах арабо-израильского конфликта.

Для анализа были выбраны следующие статьи: “*What’s the Israel-Palestine conflict about? A simple guide*” от 9.10.2023 на официальном сайте международной телекомпании *AlJazeera* (Катар) [4] и “*Timeline: Key Events In The Israel-Arab And Israeli-Palestinian Conflict”* на официальном сайте международной еврейской правозащитной организации *American Jewish Committee* (США) от 08.11.2023 [5]. Выбор данных масс-медиа обусловлен тем, что они рассчитаны на аудитории, поддерживающие противоположные стороны конфликта.

Прежде всего, следует обратить внимание на выбираемое каждым из СМИ начало хронологических рамок описываемых событий. Повествование AJC начинается с 1897 года, когда происходит собрание первого Сионистского конгресса в истории [5], тем временем объяснение истоков конфликта от AlJazeera берет начало с 1917 года, а именно письма премьера-министра Великобритании Артура Бальфура Лайонелю Ротшильду, позже известного, как

Декларация Бальфура [4]. При этом, когда в первой статье внимание читателя концентрируется на антисемитских настроениях в Европе на рубеже XIX–XX веков, проявлявшихся в виде погромов, дискриминации и насилия в сторону еврейского населения, что *«подогревало стремление к безопасной и надежной родине»* [5], AlJazeera, не упоминая о данных обстоятельствах, сразу же раскрывает содержание Декларации Бальфура, в котором британское правительство обязалась создать в Палестине «национальный очаг для еврейского народа», говоря о том, что данное письмо оказало на нее *«сейсмическое воздействие, ощущаемое по сей день»*. При этом, добавляя, что, в сущности, *«европейская страна пообещала сионистам страну с коренным 90% населением палестинских арабов»* [4], намекая на то, что интересы арабского населения были явно не учтены. Взгляд же AJC на Декларацию Бальфура довольно оптимистичен: *«это было первое признание крупной международной державой еврейских национальных устремлений.»* [5]. Итак, мы видим, с первых строк СМИ используют метод манипулирования со временем и местом подачи информации, выбирая ту точку для старта повествования, которая будет более выгодна для одной из сторон. Примечательно, что эмоциональный окрас, который придаётся Декларации Бальфура довольно контрастен и в одном случае подчёркивает ее негативные последствия, позже сказавшиеся на положении палестинцев, в другом – вполне положительные, так как документ стал явным шагом вперёд в создании израильского государства. Такой метод воздействия формирует эффект фрейминга – когнитивное искажение, при котором восприятие информации зависит от ее интерпретации: исключительно в позитивной или негативной форме [2, с. 87]. В обеих статьях, посредством подобного повествования, в котором объясняются последствия события для одной стороны, но умалчивается для противоположной, авторы способствуют формированию однобокой позиции читателя по отношению к происходящему.

Выборочное освещение тех или иных событий [2, с. 87–88] в анализируемых СМИ также отражается на том, кому отводят роли «виновника» и «жертвы» или же «героев» и «злодеев» в конфликте. Так, например, AJC, упоминает о формировании еврейской военизированной организации Хаганы для *«защиты еврейских общин от нападений местных арабов»*. Следом же говорится о резне в Хевроне в 1929 году, как о *«жестоком событии в одном из самых священных городов иудаизма»,* в ходе которого *«арабские жители совершили нападение на еврейскую общину»*. Уделяется внимание комиссии Пиля и Белой книге, *«ограничившей возможность евреев избежать Холокоста и вернуться на родину своих предков»* [5]. Из обзора AlJazeera сведения об этих событиях упускаются, но стоит указать на разницу в уровне подробностей при повествовании о событиях арабского восстания 1930-х годов, где в отличии от AJC, упоминается о том, как в ответ на забастовки палестинцев, *«обеспокоенных изменением демографической ситуацией в их стране»* британцами, сотрудничавшими с общиной еврейских поселенцев *«проводились компании массовых арестов, бомбардировки деревень и суммарные убийства, карательных сносов домов»* [4]. Статистика, касающаяся жертв конфликта, в статьях также в некоторых случаях представляется односторонне: указывается число раненных и погибших с одной стороны, не оговаривая количества жертв с другой.

Кроме того, в формировании образов «злодеев» масло в огонь подливает тщательный отбор не только событий, но и языковых средств, а также понятий и терминов, несущих негативный смысл, но постоянно находящихся на слуху у массовой аудитории, тем самым уже на подсознательном уровне вызывая отторжение. Это происходит посредством поляризации эмоционально-оценочной лексики [3, с. 96]. Что касается статей, связанных с арабо-израильским конфликтом в масс-медиа чаще всего можно столкнуться с такими понятиями, как *«антисемитизм»*, *«этническая чистка»* и анализируемые статьи на сайтах AlJazeera и AJC не являются исключением.

Теперь же определим, при каких обстоятельствах обе статьи подводят читателя к самой эскалации конфликта. Для этого сравним, как СМИ трактуют принятие Резолюции ООН № 181. Данный документ, порекомендовавший раздел Палестины на арабское и еврейское государства и стал ключевой причиной перехода конфликта в горячую стадию. В статье от AlJazeera указывается, что план был отвергнут палестинцами, *«поскольку еврейскому государству отводилось 55% территории Палестины, большую часть которых составлял плодородный прибрежный регион»* [4]. В свою очередь, AJC пишет о том, что *«еврейские лидеры принимают план раздела, в то время как арабские государства и палестинцы отвергают его»*, затем сразу же переходит к созданию Израиля, которое было встречено неприятием арабских государств, что, согласно AJC, стало причиной первой разразившейся арабо-израильской войны [5]. Таким образом, в первом случае, при виде статистических показателей и процентного соотношения раздела Палестины непринятие резолюции арабами для читателя AlJazeera становится вполне обоснованным, тогда как для читателя обзора от AJC складывается впечатление, что идея создания двух государств, которая, как, казалось бы, могла стать решением для мирного урегулирования конфликта, просто не устроило одну из сторон, без разъяснения причин.

Примечательно, что к эскалации конфликта AlJazeera подводит читателей в подзаголовке *«Накба 1948 года или этническая чистка Палестины»* [4], в нем был сделан акцент на событиях, происходивших до официального провозглашения государства Израиль, например, на трагических событиях в деревне Дейр-Ясин. В отличии от AlJazeera, где Накба больше интерпретируется как причина конфликта, массовый исход палестинцев в статье AJC упоминается уже в рамках Войны Израиля за независимость, то есть, в ходе самого конфликта и

больше трактует его уже как последствие арабо-израильской войны [5]. Очевидны манипуляция с изменением порядка фактов в тексте, а также замалчивание [1, с. 292].

Немаловажную роль помимо текстовой трактовки информации играет то, как она оформляется. AJC преподносит материал в формате вертикальной ленты времени. Шкала поделена на 3 этапа: 1897–1947; 1947–1979, 1982 – настоящее время: и от определенного года ведётся пошаговое повествование, в ходе которого мы постепенно приближаемся к событиям нынешних дней [5].

Структура статьи AlJazeera вполне схожа, она поделена на подзаголовки, а материал излагается по пунктам. Подобные способы подачи информации при котором события трактуются не «сплошным текстом», а фрагментированно, намного облегчает задачу ее фильтрации и позволяет упорядочить ход событий по своему усмотрению. В обеих статьях в ходе повествования также присутствуют ссылки на другие статьи, а также на источники других сайтов. Пожалуй, единственным отличием, дающий преимущество AlJazeera является добавление к текстовой информации визуальных материалов: диаграмм с фотографиями, а также подкрепление видео [4].

Заключение. Итак, на основе сравнения двух интерпретаций причин арабо-израильского конфликта, представленных на сайтах AlJazeera и AJC можно сделать вывод о том, что методы подачи информации обеих статей одинаковы, отличается лишь поляризованная картина событий, которая и формируется посредством этих методов. Самыми распространёнными приемом для обеих статей являются полное или частичное замалчивание, а также выборочное освещение событий, при котором учитывается о каких событиях сообщить необходимо, и какие желательно упустить, чтобы не навредить имиджу одной из сторон. Другим способом воздействия, который заметен на протяжении повествования является фрейминг при котором восприятие информации читателем зависит от того, как СМИ интерпретирует тот или иной факт в позитивном или негативном окрасе. Широко используется неровная детализация описания некоторых событий, то есть разница в уровне подробностей при их повествовании. Используется манипулирование со временем, а также местом подачи информации в тексте. Разумеется, в трактовке не обходится без использования красноречивых лексических оборотов и понятий *«безопасная, надёжная Родина»*, *«сейсмическое воздействие»*, *«жестокое событие» «забастовка жестоко подавлена»*.

Список источников и литературы:

1. Антонова О. Г. Манипуляция как феномен информационного общества // Изв. Сарат. ун-та. Новая серия. Серия: Социология. Политология. 2023. Т. 23, вып. 3. С. 289–293

2. Казаков А. А. Фрейминг медиа-текстов как инструмент воздействия на аудиторию: обзор распространенных трактовок // Изв. Сарат. ун-та. Нов. сер. Социология, Политология 2014 Т. 14, вып. 4. С 85–89

3. Пикалова Е. В. Функции оценочной лексики в СМИ в современном английском языке // Гуманитарные и социальные науки. 2022. Т. 93. № 4. С. 95–98.

4. Linah Alsaafin What's the Israel-Palestine conflict about? A simple guide 9.10.2023 [Электронный ресурс] // AlJazeera. URL: https://www.aljazeera.com/news/2023/10/9/whats-the-israel-palestine-conflict-about-a-simple-guide (дата обращения: 23.10.2025)

5. Timeline: Key Events In The Israel-Arab And Israeli-Palestinian Conflict [Электронный ресурс] // American Jewish Committee. URL: https://www.ajc.org/IsraelConflictTimeline (дата обращения: 23.10.2025).

Ростислав Олегович Исаков,
студент 4 курса механико-математического факультета Самарского университета,
E-mail: isakov.rostislav67@mail.ru

Rostislav Olegovich Isakov,
a fourth-year student at the Faculty of Mechanics and Mathematics of Samara University
E-mail: isakov.rostislav67@mail.ru

ИНСАЙДЕРСКАЯ ИНФОРМАЦИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОНЯТИЕ, ИНФОРМАЦИОННАЯ И ПРАВОВАЯ ПРИРОДА

INSIDER INFORMATION AS A THREAT TO INFORMATION SECURITY: CONCEPT, INFORMATIONAL AND LEGAL NATURE

Аннотация. Данная работа посвящена исследованию инсайдерской информации, рассматриваемой с информационной и правовой точек зрения, а также в контексте исследования угроз информационной безопасности. В рамках исследования рассматривается понятие «инсайдерская информация» в теоретических концепциях и действующем законодательстве, анализируется место инсайдерской информации в системе угроз информационной безопасности, описываются подходы к борьбе с инсайдерством в России и за рубежом. Авторы предлагают модель защиты информации от инсайдерской утечки и методику оценки инсайдерских угроз. Теоретическая ценность исследования заключается в систематизации актуальной информации по рассматриваемой проблеме с возможностью её дальнейшего применения на практике. Практическая значимость исследования состоит в возможности использования результатов для защиты конфиденциальной информации от инсайдерских угроз. Исследование способствует более глубокому анализу и пониманию угроз информационной безопасности.

Ключевые слова: инсайдерская информация, инсайдер, типы инсайдеров, инсайдерские утечки информации, информационная безопасность, методы защиты информации, модель защиты информации.

Abstract. This work examines insider information from informational, legal, and information security threat perspectives. It analyzes theoretical concepts, legislative definitions, the role of insider information within information security threats, and countermeasures against insider threats in Russia and abroad. The authors propose a model for protecting information from insider leaks and a methodology for assessing insider threats. Theoretical significance lies in systematizing relevant data for practical application. Practical value enables safeguarding confidential information against insider risks, enhancing deeper analysis of information security threats.

Keywords: insider information, insider, types of insiders, insider information leaks, information security, information protection methods, information protection model

Термин «инсайдерская информация» (англ. - inside information) в переводе означает внутреннюю информацию компании, которая недоступна широкой общественности. В российском законодательстве инсайдерская информация определяется как точные и конкретные сведения, которые не являются общедоступными; могут существенно повлиять на цены финансовых инструментов, иностранной валюты или товаров; подпадают под режим коммерческой, служебной, банковской или иной охраняемой законом тайны [1].

Ключевыми признаками инсайдерской информации являются:

1. Ограниченность доступа – информация не должна быть известна третьим лицам.
2. Точность сведений – инсайдерская информация является правдивой, в противном случае она относится к дезинформации.
3. Существенность – способность влиять на рыночные цены.
4. Конкретность – четкая привязка к определенным активам.

Примеры инсайдерской информации:

1. Планы поглощений и слияний до их публичного анонсирования.
2. Данные о грядущих изменениях в руководстве компании.
3. Результаты клинических испытаний фармацевтических компаний.
4. Информация о предстоящих аудиторских проверках или исках [2].

Современные исследования выделяют пять основных типов инсайдеров:

1. Неосторожные (более 80% случаев) действуют без злого умысла и нарушают политики безопасности по незнанию.
2. Манипулируемые становятся жертвами социальной инженерии, нередко подвергаются шантажу или давлению.
3. Оскорблённые (саботажники) – действуют из мести и обычно озлоблены в связи с недавним увольнением или конфликтом. Как цель они ставят навредить репутации компании.
4. Совместительствующий тип, такой нарушитель работает на внешнее лицо ввиду каких-либо причин (деньги, шантаж, угрозы), но не хочет в дальнейшем покидать компанию.
5. Внедренные агенты целенаправленно устраиваются в компанию, при этом работая в компании-конкуренте.

Типичные методы инсайдеров для получения необходимой информации:

1. Атака с повышением привилегий – это метод, который предоставляет инсайдеру повышенный доступ к защищенным ресурсам.

2. Эксфильтрация состоит в том, чтобы переместить конфиденциальные ресурсы из защищенной сети в личное владение.

3. Фишинговые электронные письма, с помощью которых киберпреступник-аутсайдер может воспользоваться преимуществами инсайдера.

4. Злоумышленник может воспользоваться доверием коллег для получения необходимых ему сведений [3].

Также для вычисления инсайдеров существуют технические индикаторы, исходя из которых можно предполагать о нелояльности сотрудника:

1. Печать конфиденциальных документов в нерабочее время.
2. Массовое скачивание файлов, не связанных с обязанностями.
3. Попытки доступа к закрытым разделам корпоративной сети [4].

В качестве поведенческих индикаторов могут выступить следующие факторы:

1. Внезапное проявление интереса к несвойственным темам.
2. Участившиеся запросы на доступ к дополнительным ресурсам.
3. Изменение привычных паттернов работы.
4. Конфликты с руководством [5].

Одним из приоритетных направлений регулирования инсайдерской информации является разработка моделей защиты информации и пресечения преступлений. В структуре модели защиты информации можно выделить три уровня: 1) государственные методы, 2) биржевые методы, 3) корпоративные методы.

Государственные методы относятся к компетенциям государства и Банка России как мегарегулятора. Данные методы включают разработку законодательной базы, регулирующей общественные отношения, связанные с инсайдерской информацией. Второй уровень модели регулирования инсайдерской деятельности – это биржевые методы. Для обеспечения безопасности участников рынков биржи могут устанавливать свои правила, которые не должны идти вразрез с Федеральным законодательством. Третий уровень – это методы защиты конфиденциальной информации на предприятиях и в корпорациях. В качестве примера могут выступить:

1. Разработка и внедрение политики работы с инсайдерской информацией.
2. Проверка на наличие «дыр» в информационной сфере организации.
3. Антиинсайдерская кадровая политика – методы проверки деловых качеств, социальной интеграции с обществом, умения хранить информацию, психологических и моральных устоев работников.

4. «Китайская стена» – это метод, исключающий взаимодействие работников, чьи компетенции относятся к инсайдерской информации, с работниками, которые не имеют доступа к ней.

5. Технические решения и методы, внедряемые на уровне компании.

Правовое регулирование вопроса об инсайдерской информации в России осуществляется ст. 185 пункт 6 УК РФ (до 6 лет лишения свободы)

Заключение. Таким образом инсайдерские угрозы представляют собой комплексную проблему, требующую системного подхода, сочетающего технические, организационные и правовые меры. Стоит также добавить, что предотвращение совершения противоправных действий в области инсайдерской информации эффективнее и проще, нежели расследование уже совершенных нарушений, а инвестиции в защиту от инсайдерских угроз окупаются сохранением репутации и активов.

Список источников и литературы:

1. Вавулин Д.А. Комментарий к Федеральному закону от 27 июля 2010 года № 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» [Текст]. М.: Юстицинформ. 2011. С. 216.

2. Кашкурова Т. Т. К вопросу о понятии инсайдерской информации [Текст] // Актуальные проблемы современного права в научных исследованиях молодых ученых-юристов: Сборник статей по материалам Всероссийской научно-практической конференции магистров, аспирантов и соискателей, Москва, 22 марта 2024 года. – М.: Всероссийский государственный университет юстиции, 2024. С. 67.

3. Мамочка Е. А. Типы личности преступника-инсайдера [Текст] / Е. А. Мамочка // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2016. – Т. 8, № 3(34). – С. 70-78. – EDN WMAGYP

4. Поляничко М.А. Использование технических индикаторов для выявления инсайдерских угроз [Электронный ресурс] // Кибернетика и программирование. 2018. № 6. С. 40-47. DOI: 10.25136/2644-5522.2018.6.27970 URL: https://nbpublish.com/library_read_article.php?id=27970 (дата обращения: 24.10.2025).

5. Мартьянов Е.А. Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей [Текст]: автореф. дис. ... канд. техн. наук: 05.13.19. М., 2019.

Филиппов Илья Юрьевич,
Студент группы 4443-100301D,
кафедры безопасности информационных систем,
Механико-математический факультет
Самарский национальный исследовательский
университет имени академика С. П. Королева,
E-mail: Filippov.Ilya2005@yandex.ru

Filippov I. Yurievich,
Student, Group 4443-100301D,
Department of Information Systems Security,
Faculty of Mechanics and Mathematics
Samara National Research University
named after academician S. P. Korolev,
E-mail: Filippov.Ilya2005@yandex.ru

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННОМ ОБЩЕСТВЕ

PROBLEMS OF REGULATING THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY

Аннотация. Автором раскрыты ключевые проблемы развития искусственного интеллекта: непрозрачность алгоритмов, алгоритмическая предвзятость, сложность распределения ответственности и киберугрозы. Рассмотрены проблема «черного ящика» в нейросетях, усвоение алгоритмами дискриминационных паттернов, парадокс автономных систем и использование ИИ в преступных целях. Проанализирована российская модель регулирования ИИ с гибридным подходом, сочетающим стимулирующие меры и саморегулирование. Рассмотрены методы объяснимого ИИ (XAI), стратегии выявления предвзятости, механизмы ответственности в России и международные инициативы БРИКС. Дипфейки выросли на 500% в 2025 году. Необходимо сочетание технологических решений, правовых механизмов и укрепления сотрудничества в рамках БРИКС и ШОС.

Ключевые слова: искусственный интеллект, прозрачность алгоритмов, алгоритмическая предвзятость, ответственность, киберугрозы, этика ИИ, Россия.

Abstract. The author reveals key AI development challenges: algorithmic opacity, algorithmic bias, responsibility distribution complexity, and cyber threats. The "black box" problem in neural networks, algorithms assimilating discriminatory patterns, autonomous systems operating beyond developer intent, and AI use in crime are examined. Russia's hybrid AI regulation model combining stimulating measures and self-regulation is analyzed. Explainable AI (XAI) methods, bias detection strategies, responsibility mechanisms in Russia, and international BRICS initiatives are reviewed. Deepfakes increased 500% in 2025. Trustworthy AI development requires combining technological solutions, legal mechanisms, and strengthening cooperation within BRICS and SCO.

Key words: artificial intelligence, algorithmic transparency, algorithmic bias, responsibility, cyber threats, AI ethics, Russia.

Проблема прозрачности и объяснимости решений искусственного интеллекта. Проблема «черного ящика» заключается в невозможности понять логику решений многослойных нейросетей с миллиардами параметров, что создает барьеры для доверия к искусственному интеллекту (ИИ) в критически важных сферах. Национальная стратегия определяет прозрачность как объяснимость работы алгоритмов и недискриминационный доступ пользователей к информации. Развивается направление объяснимого ИИ (*XAI*) с методами *LIME* и *SHAP* для создания упрощенных объяснений [1]. Особенно критична непрозрачность в здравоохранении, правосудии и финансах, где ошибки могут иметь катастрофические последствия. Кодекс этики в сфере ИИ от 26 октября 2021 года устанавливает принцип прозрачности как ключевой этический стандарт [3]. Российская нормативная база предлагает сочетание гибридных систем, совмещающих мощь глубокого обучения с прозрачностью классических алгоритмов, однако практическая реализация остается сложной.

Проблема юридической ответственности за действия ИИ. Российское законодательство не признает ИИ самостоятельным субъектом права. Ответственность за действия ИИ несут лица, использующие технологии: разработчики, производители, владельцы и пользователи. Сложнейшей является ситуация автономного причинения вреда современными системами с самообучением, не предусмотренным разработчиком. Федеральный закон № 258- ФЗ предусматривает возмещение вреда в соответствии с гражданским законодательством [2]. В 2024 году введено обязательное страхование гражданской ответственности участников экспериментальных режимов. Концепция подчеркивает необходимость разработки механизмов гражданско-правовой, уголовной и административной ответственности с учетом степени автономности систем [8]. Кодекс этики закрепляет, что ответственность за ИИ всегда несет человек [3].

Киберугрозы и использование ИИ в преступных целях. Использование ИИ в киберпреступности представляет растущую угрозу. В 2025 году ожидается рост мошенничества, фишинга, дипфейк-технологий и социальной инженерии. Количество инцидентов с дипфейками выросло на 500% в 2025 году [4]. Злоумышленники используют ИИ для создания продвинутого вредоносного программного обеспечения (ПО), автоматизации атак *Distributed Denial of Service*

(DDoS) и выявления уязвимостей. Указ Президента № 490 подчеркивает принцип безопасности и недопустимость использования ИИ для причинения вреда [10]. Для противодействия системы кибербезопасности применяют ИИ для обнаружения аномалий, блокирования подозрительных действий и прогнозирования угроз. Национальная стратегия предусматривает формирование комплексной системы безопасности при разработке и использовании ИИ.

Конфликт инноваций и регуляторных ограничений. Регулирование ИИ сталкивается с конфликтом между стимулированием инноваций и обеспечением безопасности. Правовая база отстает от темпов развития инновационной деятельности [5]. Закон Европейского союза (ЕС) об ИИ *(AI Act),* вступивший в силу 1 августа 2024 года, вызвал дискуссии, так как требования по раскрытию архитектуры считаются нарушением коммерческой тайны. Более 65% компаний в ЕС не уверены, смогут ли адаптироваться без значительных потерь. Крупные компании призывают отложить чувствительные положения. В России применяется гибридный подход: стимулирующие нормативные акты, точечные ограничения и саморегулирование. Закон № 258-ФЗ позволяет тестировать инновационные решения без риска нарушить законодательство. Концепция исходит из того, что ИИ не должна ограничиваться, за исключением случаев высокого риска вреда жизни и здоровью [9].

Международный опыт регулирования ИИ. Регулирование ИИ на международном уровне характеризуется отсутствием унифицированных стандартов. Более 60 стран приняли меры по регулированию ИИ, однако каждая разрабатывает собственный подход. Консультативный орган Организации Объединенных Наций (ООН) по ИИ опубликовал семь рекомендаций:

- создание международной научной группы по ИИ;
- организация политического диалога по управлению ИИ;
- центр обмена стандартами ИИ;
- глобальная сеть по наращиванию потенциала;
- глобальный фонд для ИИ;
- глобальная система данных ИИ;
- офис ИИ в Секретариате ООН.

ЮНЕСКО в 2021 году приняла Рекомендацию об этике ИИ. В марте 2024 года ООН приняла резолюцию о внедрении национальных структур управления ИИ. Казанская декларация БРИКС 2024 года обозначила признание роли ООН, создание альянса БРИКС в области ИИ и разработку этических норм. Европейский союз принял первый системный нормативный акт *AI Act*. Китай применяет трехэтапный подход: либерализация, усиление контроля и стабилизация [6].

Заключение. Регулирование ИИ осложняется конфликтом между инновациями и контролем, непрозрачностью алгоритмов, предвзятостью, сложностью распределения ответственности и киберугрозами. Российская модель основана на гибридном подходе с экспериментальными режимами и саморегулированием [7]. Необходимы комплексные меры: развитие объяснимого ИИ, методы выявления предвзятости, совершенствование механизмов ответственности, укрепление сотрудничества в рамках БРИКС и ШОС, баланс между развитием и защитой прав человека. Важно не допустить чрезмерной политизации и сохранить эту сферу как поле конструктивного сотрудничества. Необходимо разработать модельные правовые акты, гармонизировать нормативные требования и обеспечить совместимость стандартов на международном уровне.

Список источников и литературы:

1. Достижение алгоритмической прозрачности и объяснимости в системах искусственного интеллекта [Электронный ресурс] // Lawjournal.digital. URL: https://lawjournal.digital/transparency-ai/ (дата обращения: 19.11.2025).

2. Дилемма юридической ответственности ИИ. Кто несет ответственность за ошибки искусственного интеллекта? [Электронный ресурс] // Eg-online.ru. URL: https://www.eg-online.ru/article/499754/ (дата обращения: 12.11.2025).

3. Кодекс этики в сфере искусственного интеллекта (от 26 октября 2021 г.) [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QHPfU (дата обращения: 11.11.2025).

4. Кибербезопасность и искусственный интеллект [Электронный ресурс] // Falcongaze.com. URL: https://clck.ru/3QHPdP (дата обращения: 11.11.2025).

5. Конфликт инноваций и регуляторных ограничений в развитии искусственного интеллекта [Электронный ресурс] // Cyberleninka.ru. URL: https://cyberleninka.ru/article/innovation-regulation-conflict/ (дата обращения: 9.11.2025).

6. Механизмы реализации сотрудничества стран БРИКС в области искусственного интеллекта и стратегия Китая [Электронный ресурс] // e-notabene.ru. URL https://clck.ru/3QHPkL (дата обращения: 9.11.2025).

7. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права [Электронный ресурс] // cyberleninka.ru URL https://clck.ru/3QHPkL (дата обращения: 10.11.2025).

8. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в Москве» [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QHPvr (дата обращения: 11.11.2025).

9. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URLhttps://clck.ru/3QHPyV (дата обращения: 11.11.2025).

10. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») [Электронный ресурс] // КонсультантПлюс. URL: https://clck.ru/3QHPzj (дата обращения: 11.11.2025).

Кох Дмитрий Денисович,
Студент группы 4443-100301D, кафедры безопасности информационных систем,
Механико-математический факультет
Самарский национальный исследовательский университет имени С.П.Королева,
E-mail: iamthewinterchild@gmail.com

Koch D. Dmitry,
Student, Group 4443-100301D, Department of Information Systems Security,
Faculty of Mechanics and Mathematics
Samara National Research University named after S.P. Korolev,
Email: iamthewinterchild@gmail.com

ЭТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОЦЕССЕ ОБУЧЕНИЯ

ETHICAL ASPECTS OF ARTIFICIAL INTELLIGENCE USE IN THE EDUCATIONAL PROCESS

Аннотация. В работе представлены ключевые этические вызовы, сопровождающие внедрение искусственного интеллекта (ИИ) в российское образование. Особое внимание уделено вопросам защиты частной жизни, академической честности, недопущения дискриминации, трансформации роли преподавателя, а также равенству доступа и культурному многообразию. Анализируются современные отечественные исследования, отражающие взгляды и специфические проблемы сферы образования в России.

Ключевые слова: искусственный интеллект, этика, образование, доступность, индивидуализация, культурная специфика.

Abstract. The paper presents key ethical challenges accompanying the introduction of artificial intelligence (AI) in Russian education. Particular attention is paid to privacy protection, academic integrity, non-discrimination, transformation of the teacher's role, as well as equal access and cultural diversity. Contemporary domestic research reflecting views and specific problems of the education sector in Russia is analyzed.

Key words: artificial intelligence, ethics, education, accessibility, individualization, cultural specificity.

Введение. Интенсивное развитие цифровых технологий делает ИИ неотъемлемой частью современного образования. Российские научные публикации отмечают, что наряду с ростом персонализации и инклюзивности учебного процесса, внедрение ИИ в школы и вузы вызывает

комплекс этико-гуманитарных вопросов. Одна из ключевых задач – обеспечение справедливости, прозрачности и сохранения автономии личности, когда автоматизированные системы принимают решения, влияющие на образовательную судьбу человека [1].

Защита данных и конфиденциальность. Повсеместная обработка больших массивов образовательных и личных данных стала одним из главных предметов дискуссии. Участники образовательного процесса вынуждены доверять программным платформам, не всегда понимая механизмы сбора или алгоритмизацию сведений. Это требует высокой этической культуры от разработчиков и организаторов обучения. Крайне важно, чтобы цифровые системы не превращали образование в безличный, статистически управляемый процесс, а сохраняли уважение к достоинству пользователя, формировали критичность мышления и давали возможность понять логику создаваемых алгоритмов оценки результатов [2].

Академическая честность и плагиат. Массовое распространение технологий ИИ среди студентов и школьников породило новую этическую ситуацию: планка самостоятельности снизилась, а плагиат стал более трудно различимым из-за генеративных возможностей нейросетей. Российские вузы реагируют на вызовы образовательного процесса обновлением учебных программ, развитием навыков грамотного цитирования и формированием критического подхода к анализу результатов, добытых с помощью искусственного интеллекта. При этом преподавателю отводится роль не только контролёра, но и наставника в сфере этичного обращения с технологиями [3].

Равенство доступа и инклюзивность. Важнейшим социальным вызовом для страны остаётся задача обеспечения справедливой доступности качественного образования для всех категорий студентов. Российские эксперты и практики подчёркивают, что потенциал ИИ может служить инструментом снижения неравенства: интеграция автоматизированных систем, онлайн-курсов и переводчиков, адаптированных обучающих платформ, позволяет преодолеть географические, экономические и физические барьеры, а также раскрыть возможности для людей с ограниченными возможностями здоровья. Вместе с тем, нужно учитывать риски появления нового цифрового разрыва: не все учебные заведения страны имеют равные технические и финансовые ресурсы, что может, напротив, усилить социальное расслоение. Этическая задача состоит в том, чтобы внедрение ИИ не превратилось в элитарную услугу для отдельных групп, а образовало инклюзивную и равноправную среду для студентов всех регионов и социальных слоёв [4].

Культурная специфика и многообразие. Стремительный прогресс технологий ИИ в образовании, по мнению ряда российских педагогов и философов, должен сопровождаться сохранением баланса между универсальными и национальными смыслами. Искусственный

интеллект способен размывать традиционные формы внеклассной коммуникации, иногда – навязывать чужие ценности посредством предустановленных алгоритмов. Научные публикации настаивают: система образования должна быть ориентирована на признание культурного многообразия, национальных традиций и мировоззрения конкретных обучающихся. Надо избегать шаблонного «копирования» зарубежных кейсов, обеспечивая адаптацию цифровых решений к местной образовательной реальности, языковым и ментальным особенностям региона. Только такой подход способен сделать ИИ инструментом расширения личной свободы, а не средством стандартизации и внешнего контроля [5].

Роль преподавателя в эпоху ИИ. Внедрение ИИ не отрицает, а переосмысляет значение преподавателя, как основного посредника между обучающимся и смысловым потенциалом образования. Российские исследователи считают, что ИИ эффективно выполняет рутинные задачи, но не способен быть источником гуманитарной поддержки, участвовать в формировании жизненных принципов или передаче локальных ценностей. Педагог остаётся носителем культурной миссии, который интегрирует технологии, адаптируя их этично и взвешенно, – тогда цифровая среда становится пространством для творчества и роста личности, а не только для проверки стандартных знаний [6].

Заключение. Этическое сопровождение ИИ в образовании невозможно без слаженной кооперации вузов, учителей, студентов и программных разработчиков. Российские публикации подчёркивают приоритет развития цифровой грамотности всех участников процесса, просвещения по вопросам гуманистических ценностей и создания каналов обратной связи. Важно развивать критическое мышление, формировать навыки самостоятельной оценки новых технологических решений и не забывать о необходимости постоянного диалога между пользователями и проектировщиками образовательных платформ, чтобы ИИ соответствовал задачам безопасности и равенства.

Список источников и литературы:

1. Воронова Д. Ю. Этические аспекты использования технологии искусственного интеллекта в образовательной сфере [Электронный ресурс] / Д. Ю. Воронова. URL: https://clck.ru/3QHMC3 (дата обращения 10.11.2025).

2. Тимченко В. В. Этика искусственного интеллекта в образовании: вызовы и риски [Электронный ресурс] / В. В. Тимченко. URL: https://clck.ru/3QHMNK (дата обращения 10.11.2025).

3. Филимонова, И. В. Этическая сторона использования искусственного интеллекта в образовательном процессе [Электронный ресурс] / И. В. Филимонова. URL: https://clck.ru/3QHMe2 (дата обращения 10.11.2025).

4. Сысоев П. В. Этика и ИИ-плагиат в академической среде: понимание студентами вопросов соблюдения авторской этики и проблемы плагиата в процессе взаимодействия с генеративным искусственным интеллектом [Электронный ресурс] / П. В. Сысоев. URL: https://clck.ru/3QHMoT (дата обращения 10.11.2025).

5. Искусственный интеллект в высшем образовании: вызовы и перспективы революции [Электронный ресурс] // fa.ru. URL: https://clck.ru/3QHMuc (дата обращения 10.11.2025).

6. Искусственный интеллект в школе: добро или зло? [Электронный ресурс] // wciom.ru. URL: https://clck.ru/3QHN4N (дата обращения 10.11.2025).

Анастасия Геннадьевна Муренина,
студент Финансового университета при Правительстве РФ
Email: anastasiamurenina@yandex.ru

Anastasia G. Murenina,
Student of the Financial University under the Government of the Russian Federation
E-mail: anastasiamurenina@yandex.ru

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ СОЗДАНИЯ И РАСПРОСТРАНЕНИЯ ЭЛЕКТОРАЛЬНОГО КОНТЕНТА, СГЕНЕРИРОВАННОГО ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

FEATURES OF LEGAL REGULATION OF THE CREATION AND DISTRIBUTION OF ELECTORAL CONTENT GENERATED BY ARTIFICIAL INTELLIGENCE

Аннотация. В статье рассматриваются особенности правового регулирования создания и распространения электорального контента, сгенерированного искусственным интеллектом. Анализируются пробелы действующего законодательства и предлагаются пути совершенствования правового регулирования в данной сфере. Особое внимание уделяется рискам использования ИИ в избирательном процессе и мерам по противодействию манипуляциям общественным мнением.

Ключевые слова: искусственный интеллект, электоральный контент, правовое регулирование, избирательный процесс, цифровизация, дипфейки.

Abstract. The article examines the problems of legal regulation of the creation and distribution of electoral content generated by artificial intelligence. The gaps in current legislation are analyzed and ways to improve legal regulation in this area are proposed. Special attention is paid to the risks of using AI in the electoral process and measures to counter the manipulation of public opinion.

Key words: artificial intelligence, electoral content, legal regulation, electoral process, digitalization, deepfakes.

Цифровизация электорального процесса и ИИ. Стремительная цифровизация общества трансформирует все сферы жизни, включая политическую. Одним из наиболее значимых и одновременно рискованных проявлений этой трансформации стало использование технологий искусственного интеллекта в избирательном процессе. Актуальность исследования обусловлена необходимостью адаптации существующего правового поля к новым цифровым реалиям и выработки адекватных механизмов противодействия возникающим рискам.

Анализ действующего российского законодательства. Современное российское законодательство содержит ряд норм, которые в той или иной степени могут быть применены к регулированию электорального контента, созданного ИИ. Федеральный закон от 12 июня 2002 года № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» [3] и Федеральный закон от 22 февраля 2014 года № 20-ФЗ «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» [2] устанавливают базовые принципы предвыборной агитации. Однако прямого запрета на использование искусственного интеллекта для генерации агитационных материалов в этих законах нет.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4] обязывает маркировать материалы, распространяемые в интернете, которые созданы с использованием ИИ с целью распространения умышленно искаженной информации, имеющей высокую общественную значимость. Однако механизм применения этой нормы к политическому контенту, особенно в условиях быстротечной избирательной кампании, остается неочевидным [1]. Таким образом, действующее регулирование не успевает за развитием технологий искусственного интеллекта, что создает серьезные риски для электорального процесса.

Особенности правоприменения и возможные пути совершенствования регулирования. Основная проблема заключается в коллизии между необходимостью обеспечить добросовестность выборов и избежать избыточного регулирования, которое могло бы ограничить инновации и свободу слова [2]. В качестве ключевых аспектов для оптимизации правового регулирования можно предложить:

– закрепление специального запрета в избирательном законодательстве на распространение агитационных материалов, созданных с помощью, ИИ, которые имитируют реальные действия или высказывания кандидатов без их согласия;

– введение обязательной маркировки всего электорального контента, созданного с существенным использованием ИИ;

– установление четкой ответственности для кандидатов и избирательных объединений за распространение от их имени любого агитационного контента, включая сгенерированный ИИ;

– наделение избирательных комиссий и Роскомнадзора полномочиями по оперативному реагированию на факты распространения манипулятивного контента, созданного ИИ.

Заключение. Технологии искусственного интеллекта создают беспрецедентные вызовы для института свободных и честных выборов. Существующее правовое регулирование в России и большинстве других стран отстает от темпов технологического развития и не содержит специализированных норм, направленных на минимизацию рисков, связанных с генеративным ИИ в электоральном процессе. Для защиты суверенитета электорального выбора и общественного доверия необходима скорая и взвешенная модернизация законодательства. Она должна быть направлена на установление прозрачности происхождения контента, четкое определение субъектов ответственности и создание эффективных механизмов быстрого реагирования на цифровые манипуляции. Успех в этой области будет зависеть от сбалансированного подхода, сочетающего защиту демократических ценностей со стимулированием ответственного использования цифровых инноваций.

Список источников и литературы:

1. Искусственный интеллект в предвыборной агитации [Электронный ресурс] // Адвокатское бюро «АСП». 2023. URL: https://alrf.ru/articles/iskusstvennyy-intellekt-v-predvybornoy-agitatsii/ (дата обращения: 07.11.2025).

2. Федеральный закон от 22.02.2014 №20–ФЗ (ред. от 01.07.2024) «О выборах депутатов Государственной Думы Федерального Собрания Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_159349/ (дата обращения: 08.11.2025).

3. Федеральный закон от 12.06.2002 №67-ФЗ (ред. от 25.12.2023) «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_37119/ (дата обращения: 08.11.2025).

4. Федеральный закон от 27.07.2006 №149-–ФЗ (ред. от 10.07.2023) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 08.11.2025).

Секция А1

«Международное управление технологиями искусственного интеллекта: правовые, политические и этические аспекты глобальной безопасности»

Дарья Александровна Голованова,
Студент ФГБОУ ВО «КНИТУ»
Казань, Россия
Научный руководитель: Шевко Наиля Рашидовна,
кандидат экономических наук,
доцент кафедры информационной безопасности
E-mail: bowbabochka@gmail.com

Darya A. Golovanova
Student of Kazan National Research Technological University (KNITU)
Kazan, Russia
Scientific Supervisor: Shevko Nailya Rashidovna,
Candidate of Economic Sciences,
Associate Professor of the Department of Information Security
E-mail: bowbabochka@gmail.com

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ВНЕДРЕНИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

LEGAL SUPPORT FOR THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE IN THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

Аннотация. В статье рассматриваются правовые аспекты обеспечения безопасности критической информационной инфраструктуры при внедрении искусственного интеллекта. Анализируются российское законодательство и международная практика, выявляются основные риски и пробелы в регулировании. Предлагаются меры по совершенствованию правовой базы, включая сертификацию ИИ и распределение ответственности.

Ключевые слова: критическая информационная инфраструктура, искусственный интеллект, кибербезопасность, правовое регулирование, ответственность, сертификация, информационная безопасность.

Abstract. This article examines the legal aspects of ensuring the security of critical information infrastructure in the implementation of artificial intelligence. Russian legislation and international practices are analyzed, and the main risks and regulatory gaps are identified. Measures for improving the legal framework are proposed, including AI certification and the allocation of responsibilities. It is concluded that proactive legal regulation is necessary for the safe deployment of these technologies.

Key words: critical information infrastructure, artificial intelligence, cybersecurity, legal regulation, liability, certification, information security

Понятие и значение критической информационной инфраструктуры (КИИ). Федеральный закон №187-ФЗ определяет КИИ как «совокупность информационных систем и сетей связи, обеспечивающих работу стратегически важных сфер: энергетики, транспорта, банковской системы, связи, здравоохранения и промышленности» [8]. Владельцы таких объектов обязаны выявлять значимые объекты, присваивать им категории и обеспечивать комплексную защиту. Нарушение их функционирования может привести к катастрофическим последствиям. Рост числа инцидентов в последние годы, по данным ФСТЭК и Роскомнадзора, подтверждает необходимость совершенствования мер защиты и повышения устойчивости таких систем к внешним и внутренним воздействиям [1].

Роль ИИ в обеспечении функционирования КИИ. Искусственный интеллект (ИИ) активно внедряется в КИИ для:

– анализа больших массивов данных;
– прогнозирования аварийных ситуаций;
– мониторинга состояния оборудования;
– выявления кибератак и инцидентов;
– оптимизации технологических процессов.

Однако внедрение ИИ сопровождается проблемами: алгоритмы могут быть уязвимы к манипуляциям, ошибки обучения способны вызвать сбои в управлении, а зависимость от зарубежных ИИ-платформ создаёт угрозу утечки данных. Отсутствие единых требований к безопасности ИИ-систем в КИИ делает их использование потенциально опасным [4].

Нормативно-правовое регулирование КИИ и ИИ. Система регулирования строится на следующих документах:

– ФЗ №187-ФЗ «О безопасности КИИ РФ» –закрепляет принципы защиты и обязанности владельцев объектов [8];
– Доктрина информационной безопасности РФ – определяет стратегические приоритеты защиты информации [6];
– Указ Президента №490 – утверждает Национальную стратегию развития ИИ до 2030 года [5];
– Постановление Правительства №1912 – регулирует переход КИИ на доверенные отечественные программно-аппаратные комплексы [3];

– Проект ГОСТ Р «Искусственный интеллект в критической информационной инфраструктуре. Общие положения.» –вводит требования к безопасности и управлению рисками ИИ-систем [2].

Несмотря на наличие нормативной базы, она остаётся фрагментарной: отсутствует закон, регулирующий использование ИИ именно в критической инфраструктуре, а также единые стандарты аудита и сертификации ИИ [4].

Основные проблемы правового регулирования. Правовое обеспечение безопасности КИИ при использовании ИИ сталкивается с рядом проблем:

– неопределённость статуса ИИ. Законодательство не даёт чёткого определения понятия «искусственный интеллект» в контексте КИИ, что усложняет правоприменение;
– отсутствие сертификации ИИ-систем. Нет обязательных процедур оценки алгоритмов по уровню безопасности, устойчивости к кибератакам и качеству обучающих данных;
– недостаточная ответственность. Не урегулирован вопрос о том, кто несёт ответственность за ошибки или сбои в работе ИИ – разработчик, оператор или владелец системы;
– риск «чёрного ящика». ИИ может принимать решения, механизм которых непрозрачен даже для создателей. Это создаёт угрозу ошибочных действий без возможности объяснения их причин;
– зависимость от иностранного ПО. Использование зарубежных платформ ИИ повышает риск несанкционированного доступа к данным и потери технологического контроля;
– отсутствие экспертизы данных. Нормы ФЗ-152 о защите персональных данных не учитывают специфику машинного обучения, что может привести к нарушениям конфиденциальности;
– слабая интеграция стандартов. Правила ИБ для КИИ и будущие нормы по ИИ развиваются разрозненно, без унификации подходов и единого механизма контроля.

Эти проблемы формируют так называемый «регуляторный разрыв», при котором технологии ИИ развиваются быстрее, чем нормы, их регулирующие.

Пути решения и направления совершенствования законодательства. Для повышения эффективности правовой защиты КИИ при использовании ИИ необходимы системные меры:

1. разработка отдельного закона об ИИ в КИИ. В нём следует определить ключевые понятия, установить принципы безопасности, порядок сертификации и распределение ответственности;

2. создание национального реестра сертифицированных ИИ-систем. Только решения, прошедшие проверку по требованиям ФСТЭК и Росстандарта, должны допускаться к эксплуатации на объектах КИИ;

3. введение обязательной экспертизы и аудита ИИ. Необходимо проводить независимую проверку алгоритмов на устойчивость к атакам, надёжность и соответствие этическим нормам;

4. развитие отечественных технологий. Для обеспечения технологического суверенитета требуется стимулировать разработку отечественных ИИ-систем и снижение зависимости от иностранных решений;

5. повышение квалификации кадров. Специалисты КИИ должны владеть основами машинного обучения, кибербезопасности и правового регулирования ИИ;

6. международное сотрудничество. Россия должна участвовать в разработке глобальных стандартов по безопасности ИИ, чтобы интегрировать разные практики;

7. создание Центра мониторинга рисков ИИ**.** Такой орган мог бы осуществлять постоянный анализ угроз и координировать взаимодействие ведомств в сфере безопасности ИИ в КИИ.

Эти направления создадут основу для системной защиты КИИ и обеспечат баланс между инновационным развитием и безопасностью.

Заключение. Внедрение ИИ в критическую информационную инфраструктуру способствует развитию, однако при этом усиливает уязвимости. Российское законодательство безусловно адаптируется к вызовам цифровой эпохи, однако требует дальнейшего развития. Необходим комплексный подход, включающий технические, организационные и правовые меры. Только при объединении усилий государства, бизнеса и научного сообщества возможно обеспечить устойчивость КИИ и защиту национальных интересов в условиях стремительной цифровой трансформации.

Список источников и литературы:

1. Group-IB. Отчёт о киберугрозах 2025 [Электронный ресурс] // Group-IB. –2025. URL: https://www.group-ib.com/ru/landing/high-tech-crime-trends-2025/ (дата обращения: 09.11.2025).

2. Павлов Н. Новый ГОСТ изменит работу с ИИ в КИИ [Электронный ресурс] // ITSEC.RU. –2025. URL: https://www.itsec.ru/articles/novyj-gost-izmenit-rabotu-s-ii-v-kii (дата обращения: 09.11.2025).

3. Постановление Правительства РФ от 14 ноября 2023 г. № 1912 «О переходе субъектов КИИ РФ на доверенные программно-аппаратные комплексы» [Электронный ресурс] // Гарант. URL: https://www.garant.ru/products/ipo/prime/doc/407912691/ (дата обращения: 09.11.2025).

4. РБК. Аналитика о развитии цифрового регулирования КИИ и ИИ [Электронный ресурс] // RBC.ru. –2025. URL: https://www.rbc.ru/technology_and_media/02/09/2025/68b58a529a79470cf5073158 (дата обращения: 09.11.2025).

5. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс] // Кремль. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 09.11.2025)

6. Указ Президента Российской Федерации от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Кремль. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 19.12.2025).

7. Указ Президента РФ от 27 декабря 2021 г. № 755 «О развитии технологий искусственного интеллекта и о внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490» [Электронный ресурс] // Кремль. –Режим доступа: http://www.kremlin.ru/acts/bank/51814 (дата обращения: 09.11.2025).

8. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 09.11.2025).

Зогранян Евгений Владленович,
аспирант Российской академии народного хозяйства
и государственной службы при Президенте РФ,
E-mail: zogranyane@mail.ru

Eugen V. Zogranyan,
Postgraduate student at the Russian Presidential Academy
of National Economy and Public Administration,
E-mail: zogranyane@mail.ru

ОПРАВДАННОСТЬ ИСПОЛЬЗОВАНИЯ ИИ В ПОЛИТИЧЕСКИХ ЦЕЛЯХ

USE OF AI FOR POLITICAL PURPOSES

Аннотация. Автором рассмотрены основные современные направления использования ИИ в политических целях, а также выдвинута гипотеза относительно вероятной причины возникновения неумышленного искажения в результатах работы алгоритмов ИИ.

Ключевые слова: искусственный интеллект, субъектность ИИ, манипулятивное воздействие, политическая стабильность.

Abstract. The author examines the main contemporary uses of AI for political purposes and proposes a hypothesis regarding the likely cause of unintentional bias in the results of AI algorithms.

Key words: artificial intelligence, AI subjectivity, manipulative influence, political stability.

Развитие ИКТ заставляет серьезно задуматься о том потенциале, который может стоять за дальнейшей разработкой и усовершенствованием ИИ, нельзя полностью исключать вероятность возникновения общего искусственного интеллекта (AGI) [9] и достижение новых рубежей в вопросе прогресса усовершенствования ИИ вероятно является вопросом времени.

Согласно «закону плотности больших моделей», максимальная плотность возможностей больших языковых моделей (LLM) экспоненциально увеличивается со временем [1], что делает возможным достижение высоких показателей не только за счет вклада лабораториями по разработке ИИ все больших сумм в вычисления, необходимые для обучения своих моделей, но и частично обходить такого рода сценарии в условиях санкционного давления, как продемонстрировал Китай.

Сама тема использования ИИ во многих областях современного мира за последние годы стала настолько популярной, что может сравниться с «пузырем доткомов», при этом хотелось бы отметить, что стоит аккуратно подходить к прогнозированию социальных и политических

последствий внедрения ИИ во всем его многообразии. Автор данной статьи предлагает рассмотреть данный вопрос с точки зрения политических процессов современного государства.

В качестве широко известных примеров использования ИИ в политических целях можно рассмотреть федеральные выборы в Австралии, в ходе которых ряд политических партий активно использовали искусственный интеллект для создания контента политического характера, например Либеральная партия Австралии выпустила видео полностью сгенерированное ИИ относительно высоких цен на бензин [5]. При этом не только крупные партии использовали ИИ, например независимый кандидат Деб Леонард записала агитационное музыкальное видеообращение с применением автотюна [4] для привлечения молодого поколения избирателей, что тоже можно считать как использование искусственного интеллекта.

Такого рода примеры демонстрируют, как ИИ все более часто становится частью современных политических стратегий под предлогом налаживания более эффективного взаимодействовать с избирателями. Какова результативность таких попыток пока не до конца понятно, есть примеры как успешного применения ИИ, так и нет. На данный момент такого рода видео могут становится популярным не столько по причине наличия большого количества сторонников кандидата, сколько просто в силу пока еще диковинности таких видео и активной популяризации ИИ для повышения стоимости акций ряда компаний, связанных с производством «железа».

Более целесообразным является обратить внимание на то, что как простой искусственный интеллект, так и общий искусственный интеллект в случае его возникновения, может быть использован для манипулирования общественным мнением. При этом даже в случаях, не подразумевающих злонамеренное использование, сложность алгоритмов модели и несовершенство логики запроса может приводить к ошибкам в расчете последствий и в определенном смысле опережать нормативные рамки, что косвенно может влиять на эффективность работы социальных и политических институтов.

Сегодня большая часть общедоступных отечественных и зарубежных моделей используют защиту от сценариев явно злонамеренного использования, а варианты обхода защиты постоянно исключаются по мере их нахождения, однако как было сказано выше, модели при правильной постановке запроса в силу эффекта «Китайской комнаты» могут оказывать помощь в планировании и подготовке противоправных действий. Теоретически в случае возникновения общего искусственного интеллекта эта задача потребует больше усилий для ее решения, при этом уже сегодня согласно собственной оценке безопасности OpenAI своей модели o1, риски связанные с использованием уязвимости более сложной системы возрастают [7]. Можно предположить, что по мере того, как ИИ будет внедрятся в политические процессы и его

воздействие будет становится все более общим, зависимость от него будет расти, постепенно размывая грань между принятием решений человеком и машиной, что потенциально может подрывать «субъектность» людей, тем самым переходя в область этики и даже философии. В любом случае не только политическая манипуляция представляет опасность, но и косвенные последствия применения ИИ в политических целях. Даже в вопросах, где как нам кажется ответственность субъектна, работа ИИ может не соответствовать намерениям его человеческих разработчиков или операторов, причиняя непреднамеренный вред. Например, вследствие оптимизации понятий конечной цели могут не учитываться определенные этические вопросы. OpenAI повысила оценку рисков o1, так как модель «иногда_инструментально подделывал выравнивание во время тестирования», тем самым умышленно предоставляя неверную информацию, чтобы обмануть пользователей [8].

Помимо «умышленного» обмана созданного смой моделью, было замечена тенденция генерации политического контента предвзятого характера [10]. Наиболее заметно это в странах, где есть четкое разделение на сторонников и противников определенных политических партий, например в США подразумевается противопоставление либералов и консерваторов, что отлично подходит для гипотетического примера. И если факты выдачи заведомо ложной информации известны уже дано, то погрешности в выдаче результатов политического характера для нас представляют дополнительный интерес.

Можно выдвинуть гипотезу, что погрешности и искажения в работе ИИ являются не следствием процесса обучения модели, а корни данного феномена скрыты в когнитивных искажениях самого человека как существа мыслящего.

Относительно недавние исследования в этой области показали, что такого рода искажения восприятия ИИ могут быть использованы для манипулятивного воздействия [3]. При этом также для манипулятивного воздействия можно использовать и факт генерации заведомо предвзятого политического контента [6], что косвенно может повлиять на политические предпочтения обычных пользователей за счет более частой генерации и выдачи контента определенной политической направленности.

Тонкая настройка языковых моделей и избирательность в массивах данных для обучения может стимулировать формирование определенных политических предпочтений в генерируемом контенте, что суммарно с подстройкой под субъективные предпочтения пользователя выстроенные на основе предварительно собранной и обработанной персональной информации, может дать качественной новый инструмент политической манипуляции и дезинформации. Важно отметить, что относительно недавно существовавшая проблема вероятности понимания пользователем факта ведения переписки с ИИ уже не существует, если, конечно, мы говорим про

крупные языковые модели, как например Google Gemini или последние модели от OpenAI, сегодня большинство моделей позволяют адаптировать ответы к предпочтениям отдельных пользователей, включая группы пользователей, например сторонники или противники определенных политических взглядов.

Еще одной особенностью, связанной с подстройкой под предпочтения пользователя или группы пользователей является формирование своего рода воображаемого сообщества, виртуально смоделированной общности пользователей, которая не может быть четко разграничена опираясь на созданный на основе персональных данных виртуальный профиль пользователя, грань как таковая не сколько подвижна, сколько вопрос целесообразности и ресурсоемкости процесса переубеждения решает где будет проходить линия раздела. Можно предположить, что при достаточно детальном профиле пользователя становится возможным с высоко долей вероятности просчитать сколько нужно затратить времени и ресурсов на изменение точки зрения пользователя с учетом данных о среднем времени пользования цифровой платформой и тем зонтиком платформ, которыми пользуется пользователь, например Google может использовать целый комплекс цифровых платформ для сбора персональных данных и обратной реакции. Если пользователь не попадает в какие-то неординарные условия, то ежедневный сценарий или недельный цикл использования цифровых платформ практически не изменяется, что потенциально дает возможность просчитать сколько нужно потратить ресурсов для работы с конкретным пользователем. При этом стоит также упомянуть, что в одном из последних патентов [2] компании Oracle говорится о технологии позволяющей более эффективно работать в области моделирования вероятного поведения пользователей и соответственно более качественно влиять на это поведение.

Таким образом можно сделать вывод, что вопрос борьбы за информационное пространство нисколько не замедляется, а скорее наоборот является перспективным направлением работы как технических специалистов, так и ученых в области гуманитарных наук. Также можно предположить, что широкое применение ИИ в политических целях может привести к повышению уровня политической дестабилизации. Независимо от того, как именно будет использоваться ИИ, сам факт его использования может способствовать росту нестабильности, поскольку различные политические игроки будут бороться за доминирование в этой области. Такого рода конкуренция может привести к обострению внутренней напряженности за счет либо вышеуказанных факторов, либо за счет умышленного недобросовестного использования ИИ в политических целях, стремление к превосходству в этой области рискует спровоцировать, а не сдержать нестабильность.

К наиболее вероятным мерам снижения данной угрозы автор относит:

– развитие осведомленности пользователей;
– четкое юридическое регулировать работы ИИ;
– открытость и подотчетность алгоритмов обучения ИИ;
– запрет субъектности ИИ в политической сфере.

Заключение. Несовершенство когнитивных процессов человека как существа вероятно может замедлить процесс развития эффективных методов манипулятивного воздействия. В силу сложности как самого мышления, так и тех закономерностей мышления, которые в ряде случаев нарушаются, мы пока не можем разработать инструменты точного прогнозирования поведения большого количества пользователей хотя бы в среднесрочной перспективе. Это именно тот случай, когда уязвимость становится преимуществом.

Список источников и литературы:

1. Densing Law of LLMs [Электронный ресурс]. URL: https://arxiv.org/html/2412.04315v2 (дата обращения 26.10.2025).
2. EVICTION OF WEAKLY CORRELATED SIGNALS FROM COLLECTIONS [Электронный ресурс]. URL: https://patents.google.com/patent/JPWO2021113044A5/en&dq=WO%202015199764%20A1&hl=nl&sa=X&ved=0ahUKEwjIo73st9zXAhWQ4qQKHfk5D88Q6AEIJzAA (дата обращения 26.10.2025).
3. Hackenburg K, Margetts H. Evaluating the persuasive influence of political microtargeting with large language models. [Электронный ресурс]. URL: https://pubmed.ncbi.nlm.nih.gov/38848300/ (дата обращения 26.10.2025).
4. Independent candidate drops awkward rap video to win over voters [Электронный ресурс]. URL: https://www.canberratimes.com.au/video/viral/x9hnb9w/independent-candidate-drops-awkward-rap-video-to-win-over-voters/ (дата обращения 26.10.2025).
5. The Liberal Party release a new election campaign video made entirely with AI [Электронный ресурс]. URL: https://www.theaustralian.com.au/breaking-news/the-liberal-party-release-a-new-election-campaign-video-made-entirely-with-ai/news-story/61646660ca385d4a514a98e521f4cf73 (дата обращения 26.10.2025).
6. Motoki, F., Pinho Neto, V., & Rodrigues, V. (2024). More human than human: Measuring ChatGPT political bias. [Электронный ресурс]. URL: https://www.researchgate.net/publication/373188439_More_human_than_human_measuring_ChatGPT_political_bias (дата обращения 26.10.2025).
7. OpenAI o1 System Card [Электронный ресурс]. URL: https://openai.com/index/openai-o1-system-card/ (дата обращения 26.10.2025).
8. OpenAI, “OpenAI o1 System Card,” September 12, 2024, p. 10.

9. Understanding and Benchmarking Artificial Intelligence: OpenAI's o3 Is Not AGI [Электронный ресурс]. URL: https://arxiv.org/abs/2501.07458 (дата обращения 26.10.2025).
10. Uwe Messer How do people react to political bias in generative artificial intelligence (AI)? [Электронный ресурс]. URL: https://www.sciencedirect.com/science/article/pii/S2949882124000689 (дата обращения 26.10.2025).

Павел Александрович Карасев,
к.полит.н., с.н.с., Национальный исследовательский институт мировой экономики и международных отношений имени Е. М. Примакова Российской академии наук
E-mail: karpaul@iisi.msu.ru

Pavel A. Karasev
Ph.D. (Political science), Senior Researcher Primakov National Research Institute of World·Economy and International Relations, Russian Academy of Sciences
E-mail: karpaul@iisi.msu.ru

ВОЕННО-ПОЛИТИЧЕСКИЕ АСПЕКТЫ В КОНТЕКСТЕ ГЛОБАЛЬНОГО РЕГУЛИРОВАНИЯ ИИ

MILITARY-POLITICAL ASPECTS IN THE CONTEXT OF GLOBAL AI GOVERNANCE

Аннотация. На фоне отсутствия международного консенсуса по вопросу необходимости, а также возможных форм регулирования военного использования ИИ, вызывает опасения создание новых, не инклюзивных специализированных и общих площадок для обсуждения тематики регулирования ИИ в военной сфере. При этом, идет продвижение соответствующих инициатив, которые в перспективе могут привести к навязыванию международному сообществу решений, обслуживающих узкие политические интересы отдельных стран и групп государств.

Abstract. Given the lack of international consensus on the necessity and possible forms of regulation of the military use of AI, the creation of new, non-inclusive, specialized and general forums for discussing AI regulation in the military sphere raises concerns. At the same time certain initiatives are being promoted that could potentially lead to the imposition on the international community of decisions that serve the narrow political interests of individual countries and groups of states.

Ключевые слова: международная информационная безопасность, смертоносные автономные системы вооружений, Пакт во имя будущего, ООН.

Key words: international information security, lethal autonomous weapon systems, Pact for the Future, UN.

Регулирование технологий искусственного интеллекта (ИИ) является быстро развивающейся проблематикой как на международном, так и на национальном уровне. По многим причинам регулирование использования ИИ в военной сфере является самостоятельным направлением – немаловажным фактором является наличие прочного международно-правового

фундамента в виде Конвенции о негуманном оружии [9]. В частности, Конвенция регламентирует, необходимость проведения правовых обзоров всех разрабатываемых оружейных систем, в том числе с ИИ, на предмет соблюдения её положений и норм международного гуманитарного права (МГП). В рамках докладов Группы правительственных экспертов ООН по новым технологиям в сфере создания смертоносных автономных систем вооружений (ГПЭ по САС) неоднократно подтверждалось, что существующее международное право, в том числе МГП, полностью применяется к системам вооружений с использованием ИИ. В 2019 г. Группой были впервые согласованы и приняты руководящие принципы [8], которые способствуют сближению позиций по самым острым вопросам в данной области. В то же время можно отметить отсутствие полного консенсуса. Существуют три основных взгляда на регулирование. Первый говорит о достаточности текущих механизмов, второй – о необходимости заключения специальных международно-значимых актов, а третий – о полном запрете САС.

На фоне отсутствия среди стран мира общего мнения относительно необходимости и форм регулирования ИИ, для выявления вектора развития этой проблематики важен непрерывный мониторинг и анализ обсуждений, в том числе проходящих на альтернативных площадках.

Обзор инициатив в области регулирования ИИ – военные аспекты

Исчерпывающий взгляд России на проблематику регулирования использования ИИ в военной сфере содержится в позиционном документе, включенном в доклад Генерального секретаря ООН «Применение искусственного интеллекта в военной области и его последствия для международного мира и безопасности» [7]. ГПЭ по САС названа оптимальной международной площадкой для «рассмотрения между государствами вопросов, связанных с применением технологии ИИ в военных целях» [Там же, С. 88]. При этом указано на контрпродуктивность «[переноса] проблематики применения технологии ИИ в военных целях на любые другие международные площадки… её [обсуждения] в узком составе, без участия подавляющего большинства государств-членов ООН…» [Там же, С. 92] Принципиально важно и то, что «рассмотрение вопросов военного применения ИИ в рамках Группы имеет широкий охват, не сводится сугубо к проблематике САС и затрагивает ряд важных аспектов… связанных с задействованием данной технологии в военных целях» [Там же, С. 88]. Россия считает, что текущие механизмы регулирования достаточны, а снятие озабоченностей в отношении САС «лежит в плоскости добросовестного выполнения уже действующих международно-правовых норм» [Там же, С. 89].

В отношении мест продвижения новых сомнительных инициатив, которые прямо или косвенно относятся к регулированию военного ИИ, особо выделяется площадка ООН.

В 2023 г. был создан Консультативный орган высокого уровня по искусственному интеллекту ООН. В его итоговом докладе 2024 г. отмечено, что «120 государств–членов [ООН] поддерживают новый договор по автономному оружию, и как Генеральный секретарь, так и президент Международного комитета Красного Креста призвали завершить переговоры по такому договору к 2026 году» [11, СС. 35-36]. Консультативный орган фактически продвинул эту идею, которая учитывает не все точки зрения.

Также определенное беспокойство вызывает рекомендация выработать общее понимание в отношении «механизмов тестирования, оценки, проверки и валидации» военных систем ИИ. В совокупности с идеей сотрудничества для содействия «ответственному управлению жизненным циклом систем ИИ в сфере безопасности и военной области» и создания механизмов контроля для предотвращения приобретения мощных и потенциально автономных систем ИИ опасными негосударственными субъектами [Там же], это предложение в перспективе может лечь в основу предвзятых механизмов, которые смогут «назначать» виновных в «безответственном» использовании военного ИИ, а затем – оказывать на них всестороннее давление. Известным примером такого подхода является злоупотребление США нормами, правилами и принципами ответственного поведения государств, выработанными Группой правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в 2015 г., для объявления России, Китая, Ирана и Северной Кореи злонамеренными акторами в киберпространстве и продвижения политики «сдерживания» [5].

Осенью 2024 г. в ООН был представлен Пакт во имя будущего [10]. Россия дистанцировалась от консенсуса по этому документу и его приложениям. В отношении военного использования ИИ в Пакте содержится призыв «в срочном порядке провести обсуждения, касающиеся смертоносных автономных систем вооружений, в рамках [ГПЭ по САС], с целью разработать документ, не предрешая его характер, и другие возможные меры по решению проблемы новейших технологий в сфере создания [САС]…» [Там же, С. 26] Этот призыв также несовместим с позицией России.

В феврале 2025 г. состоялся Саммит по вопросам действий в области искусственного интеллекта, на котором было принято Заявление об инклюзивном и устойчивом искусственном интеллекте для людей и планеты [1]. Несмотря на то, что в документе прямо сказано, что он относится только к гражданскому использованию ИИ, подписанты выразили поддержку другим международным форумам по регулированию ИИ, а также подчеркнули, среди прочего, необходимость глобального анализа вопросов соблюдения международного права, включая

гуманитарное право – а эта тематика, несомненно, является частью обсуждений военного использования ИИ.

Наиболее серьёзной угрозой уже устоявшимся механизмам являются Саммиты по ответственному применению ИИ в военных целях, которые проводились в 2023-2024 гг. Решением Саммита 2023 г. создана неинклюзивная Глобальная комиссия по ответственному искусственному интеллекту в военной сфере (GC REAIM). В сентябре 2025 г. она представила «Стратегическое руководство по рискам, возможностям и управлению искусственным интеллектом в военной сфере» [4], где отмечено, что приоритетом в процессах глобального управления должно стать дальнейшее развитие многосторонних подходов к обсуждениям вопросов ИИ в военной сфере. Практика реализации многосторонних подходов на других площадках, таких, как ICANN, говорит о том, что большинство будет сформировано за счет включения прозападных коммерческих и некоммерческих структур. В планах на третий Саммит – переход от Программы действий к Плану действий, то есть операционализация и отмежевание проблематики управления военным ИИ от институтов ООН.

Заключение. Стремление государств к использованию ИИ в военной сфере должно сопровождаться осознанием и осмыслением новых вызовов и угроз, однако в последние годы можно наблюдать крайнюю политизацию этого вопроса и эволюцию подходов отдельных государств, которая нарушает статус-кво.

Так, Соединенные Штаты, взгляды которых на вопрос достаточности текущих норм международного права для регулирования военного ИИ долгие годы были совместимы с позицией России, в 2023-2025 гг. представили в ГПЭ по САС т.н. «Проекты статей об автономных системах оружия – запреты и другие меры регулирования на основе международного гуманитарного права» [2]. Фактически предлагаются не новые нормы, а разъяснения и указания, как применять существующие. В ходе Саммита по ответственному применению ИИ в военных целях 2023 г., США представили созвучную этому документу «Политическую декларацию об ответственном военном использовании искусственного интеллекта и автономности» [3], которая позиционируется уже в качестве нормативной базы, регулирующей использование этих возможностей в военной сфере, и направлена на формирование международного консенсуса вокруг западных подходов.

Приведенные факты подтверждают позицию России, что новые, неинклюзивные форумы «призваны подменить реальную дискуссию между государствами на профильных площадках по вопросам «военного» ИИ, выработать в узком кругу некие понимания и стандарты в данной области. Впоследствии имеется в виду попросту поставить международное сообщество перед фактом наличия неких «келейных» договоренностей и предложить их формально утвердить» [6].

Одновременно важно подчеркнуть, что, во-первых, платформа ООН и её институты активно используются для продвижения инициатив, противоречащих позиции России, и появляются всё новые площадки для обсуждения, которые солидаризируются между собой; во-вторых, страны, которые ранее выступали или против регулирования, или за запрет САС являются или авторами (США), или подписантами (Израиль, Австрия) новых инициатив.

С учетом текущей обстановки, одним из возможных способов продвижения и защиты позиции России может стать альтернативная инициатива, направленная на разъяснение того, как международное право и МГП применимо к использованию ИИ в военных целях, которая может быть представлена на дружественных региональных и трансрегиональных площадках.

Список источников и литературы:

1. AI Action Summit: Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet // Dig.Watch [Official website], URL: https://dig.watch/resource/ai-action-summit-statement-on-inclusive-and-sustainable-artificial-intelligence-for-people-and-the-planet

2. Draft articles on autonomous weapon systems – prohibitions and other regulatory measures on the basis of international humanitarian law ("IHL"), CCW/GGE.1/2025/WP.7, 3 September 2025 // UN [Official website], URL: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2025)/CCW-GGE.1-2025-WP.7.pdf

3. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, November 9, 2023 // US Department of State [Official website], URL: https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/

4. Responsible by Design Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain, September 2025 // The Hague Centre for Strategic Studies [Official website], URL: https://hcss.nl/wp-content/uploads/2025/09/GC-REAIM-Strategic-Guidance-Report-Final-WEB.pdf

5. The National Cyber Strategy of the USA, 2019 // Trump White House [Official website], URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

6. Выступление заместителя руководителя делегации Российской Федерации, заместителя директора Департамента по вопросам нераспространения и контроля над вооружениями МИД России К.В.Воронцова в ходе тематической дискуссии по разделу V «Другие меры разоружения и международная безопасность» в Первом комитете 80-й сессии ГА ООН, Нью-Йорк, 27 октября 2025 года // МИД России [Официальный сайт], URL: https://www.mid.ru/ru/foreign_policy/news/2056224/

7. Доклад Генерального секретаря ООН *Применение искусственного интеллекта в военной области и его последствия для международного мира и безопасности*, A/80/78, 5 июня 2025 г. // ООН [Официальный сайт], URL: https://docs.un.org/ru/A/80/78

8. Доклад сессии 2019 года Группы правительственных экспертов по вопросам, касающимся новых технологий в сфере создания смертоносных автономных систем вооружений, CCW/GGE.1/2019/3, 25 сентября 2019 г. // ООН [Официальный сайт], URL: https://documents.un.org/api/symbol/access?j=G1928571&t=pdf&i=CCW/GGE.1/2019/3_9855470

9. Конвенция о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие (Конвенция о «негуманном» оружии – КНО, открыта к подписанию 10 апреля 1981 г. // МИД России [Официальный сайт], URL: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/obychnye_vooruzheniya/1413307/

10. Резолюция, принятая Генеральной Ассамблеей 22 сентября 2024 года 79/1. Пакт во имя будущего // ООН [Официальный сайт] URL: https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf

11. Управление искусственным интеллектом в интересах человечества: Заключительный доклад // ООН [Официальный сайт], URL: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_ru.pdf

Екатерина А. Макеева,
студент направления «Международные отношения и внешняя политика»
Иркутский Государственный Университет,
E-mail: kate1928@icloud.com

Татьяна В. Мацаева,
студент направления «Международные отношения и внешняя политика»
Иркутский Государственный Университет,
E-mail: matsaeva.tatyana.off@gmail.com

Ekaterina A. Makeeva,
International Relations and Foreign Policy Student
Irkutsk State University,
E-mail: kate1928@icloud.com

Tatiana V. Matsaeva,
student of International Relations and Foreign Policy
Irkutsk State University,
E-mail: matsaeva.tatyana.off@gmail.com

УКОРЕНЕНИЕ СОЦИАЛЬНОЙ ДИСКРИМИНАЦИИ В АЛГОРИТМАХ ИИ: АНАЛИЗ РАСОВОГО И ГЕНДЕРНОГО УКЛОНА

THE ROOTING OF SOCIAL DISCRIMINATION IN AI ALGORITHMS: AN ANALYSIS OF RACIAL AND GENDER BIAS

Аннотация. В статье раскрывается проблема воспроизводства и усиления социальной дискриминации в алгоритмах искусственного интеллекта. Авторы анализируют природу и механизмы возникновения расового и гендерного уклонов, рассматривая ключевые факторы: предвзятость данных, ошибки при обучении моделей и «эффект обратной связи». На реальных кейсах (COMPAS, Amazon Rekognition, рекрутинговый инструмент Amazon) демонстрируются социально опасные последствия алгоритмической предвзятости в сферах правосудия, трудоустройства и правоохранительной деятельности. В заключении предложен комплексный подход к преодолению дискриминации, сочетающий технические меры (аудит алгоритмов), этико-правовое регулирование (переход от «мягкого права» к «жесткому») и социальные изменения (разнообразие в командах разработчиков).

Ключевые слова: искусственный интеллект, алгоритмическая дискриминация, расовый уклон, гендерный уклон, предвзятость данных, этика ИИ, справедливость алгоритмов.

Abstract. The article reveals the problem of reproduction and intensification of social discrimination in artificial intelligence algorithms. The authors analyze the nature and mechanisms of racial and gender bias, considering key factors: data bias, errors in model training, and the "feedback effect." Real-world cases (COMPAS, Amazon Rekognition, Amazon recruitment tool) demonstrate the socially dangerous consequences of algorithmic bias in the fields of justice, employment, and law enforcement. In conclusion, a comprehensive approach to overcoming discrimination is proposed, combining technical measures (algorithm audit), ethical and legal regulation (transition from "soft law" to "hard law") and social changes (diversity in development teams).

Key words: artificial intelligence, algorithmic discrimination, racial bias, gender bias, data bias, ethics of AI, fairness of algorithms.

Внедрение технологий искусственного интеллекта (ИИ) в ключевые социальные сферы, от правосудия до трудоустройства, всё чаще сопровождается дискуссиями об их объективности. Распространённое представление об алгоритмах как о нейтральных и беспристрастных инструментах является глубоким заблуждением, которое маскирует серьёзные этические и правовые риски. На практике системы ИИ, обучаясь на определенных данных, отражающих существующие в обществе предубеждения, не только воспроизводят, но и усиливают социальное неравенство. В связи с этим представляется необходимым рассмотреть теоретические основы данного явления, чтобы понять его природу и механизмы действия.

Алгоритмическая дискриминация определяется как «принятие ошибочных решений в отношении конкретных лиц на основе алгоритмов» [5], которые могут дискриминировать людей по признакам пола, расы, национальности и вероисповедания. Данное явление создаёт прямую угрозу равенству (одному из основополагающих концептов правового государства). С этической точки зрения, эта проблема заставляет общество «осмысливать границы допустимого и определять» [6] меру ответственности за внедрение технологий, способных нарушать права человека.

Важно разграничивать алгоритмическую дискриминацию от смежных понятий. Если социальная дискриминация представляет собой неравное обращение с индивидами на основе их принадлежности к определённой группе, то системная и структурная дискриминация описывают более глубокие процессы, укоренённые в правилах, политиках и практиках социальных институтов. Алгоритмическая предвзятость является современным технологическим проявлением именно системной дискриминации, поскольку она встраивает исторически сложившееся неравенство в автоматизированные системы принятия решений, делая его незаметным и сложно оспариваемым.

Воспроизводство и усиление неравенства в системах ИИ происходит посредством нескольких взаимосвязанных механизмов.

Во-первых, ключевым фактором является неполнота и предвзятость данных, используемых для обучения моделей. Алгоритмы обучаются на исторических данных, которые неизбежно отражают существующие в обществе стереотипы и диспропорции. Предрассудки прошлого ведут к предрассудкам в будущем. Если в данных определённые группы населения исторически были представлены недостаточно или в искажённом свете, ИИ усвоит эти закономерности как объективную реальность.

Во-вторых, значительную роль играют ошибки при обучении моделей и роль разработчиков. ИИ не является автономным моральным агентом, поскольку не обладает субъектностью, необходимой для принятия этически взвешенных решений. Ответственность за «моральные риски разработки и внедрения» полностью лежит на людях, которые создают и пользуются этими системами. Корпоративные интересы также могут влиять на конечный результат; например, стремление к быстрой автоматизации процессов, как в случае с планами Amazon по массовому внедрению ИИ, может приводить к игнорированию этических аспектов ради экономической эффективности.

В-третьих, возникает так называемый «эффект обратной связи» (feedback loop), при котором алгоритмы не просто отражают, а активно усиливают существующие стереотипы. Например, алгоритм прогнозирования преступности, обученный на данных о более частых арестах в районах проживания расовых меньшинств, будет рекомендовать направить туда больше полицейских патрулей. Это, в свою очередь, приведёт к увеличению числа арестов в этих же районах, что создаст новые данные, «подтверждающие» исходную предвзятость алгоритма. Таким образом, система входит в замкнутый цикл, закрепляя и легитимизируя дискриминационные практики. Изучение реальных кейсов является одним из лучших способов для понимания подобных «этически неоднозначных последствий».

Критически важно понимать, что технология ИИ не является нейтральной. Она представляет собой продукт общества, отражающий его исторические, культурные и политические реалии. Алгоритмы и модели данных не существуют в вакууме; они встроены в социальный контекст, который определяет, какие данные собираются, как они интерпретируются и для каких целей используются.

Проблема усугубляется глобальным неравенством, в частности доминированием западных наборов данных. Большинство широко используемых датасетов для обучения ИИ собираются в странах Северной Америки и Европы, что приводит к недостаточной представленности других регионов и культур. Модели, обученные на таких данных, плохо работают применительно к другим группам населения, что создаёт цифровой разрыв и закрепляет существующие дисбалансы на глобальном уровне.

Одним из наиболее документированных и социально опасных проявлений алгоритмической предвзятости является расовый уклон. Системы искусственного интеллекта, всё глубже интегрируемые в критически важные общественные сферы (от правосудия и правоохранительной деятельности до трудоустройства и кредитования) демонстрируют систематические и предсказуемые ошибки, которые непропорционально негативно сказываются на расовых и этнических меньшинствах. Эти сбои не являются случайными аномалиями или неизбежной погрешностью, а представляют собой прямое технологическое следствие укоренившихся в обществе предубеждений, которые алгоритмы не только впитывают, но и многократно усиливают под маской объективного машинного анализа. Данное явление требует детального и критического рассмотрения, поскольку оно не просто подрывает доверие к технологиям, но и несёт прямую угрозу фундаментальным правам и свободам человека, закрепляя несправедливость в цифровой инфраструктуре будущего.

Истоки расовой предвзятости в ИИ лежат в самой основе машинного обучения – в данных, на которых оно строится. Алгоритмы учатся на уже имеющихся датасетах, которые являются не чем иным, как оцифрованными рассказами нашей социальной реальности со всеми её недостатками. Как утверждается в докладе Управления Верховного комиссара ООН по правам человека, технология рискует стать мощным инструментом, который будет «поддерживать исторически сложившиеся предубеждения», создавая таким образом порочный круг, где «предрассудки прошлого ведут к предрассудкам в будущем» [10]. Историческое неравенство, отражённое в статистике арестов, судебных приговоров, решениях о найме или выдаче кредитов, кодируется в данных и воспринимается машиной не как следствие системной дискриминации, а как объективная и подлежащая воспроизводству закономерность. В условиях, когда технологические гиганты, такие как Amazon, объявляют о планах по масштабному внедрению ИИ и сокращению тысяч сотрудников ради повышения эффективности, риски от неконтролируемого применения таких предвзятых систем многократно возрастают.

Проявления расового уклона многообразны и затрагивают множество областей, где решения ИИ имеют далеко идущие последствия:

Системы распознавания лиц. Эта технология стала одним из самых ярких примеров расовой предвзятости. Многочисленные исследования, включая работу проекта «Gender Shades» от MIT Media Lab [7], неопровержимо доказали, что ведущие коммерческие системы распознавания лиц значительно чаще ошибаются при идентификации людей с тёмным цветом кожи и женщин, в особенности темнокожих женщин. Погрешность для этой группы может быть в десятки раз выше, чем для белых мужчин. Это приводит к реальным трагическим последствиям, таким как неправомерные аресты на основе ложной идентификации. Дело российского учёного-

гидролога, который был ошибочно идентифицирован системой как подозреваемый в совершении преступления двадцатилетней давности, является показательным примером таких последствий, которые чуть не стоили человеку свободы [6]. Подобные случаи дискредитируют саму идею использования ИИ в правосудии и демонстрируют опасность делегирования критически важных решений несовершенным технологиям.

Алгоритмы, используемые для прогнозирования преступлений (predictive policing), являются ещё одной областью высокого риска. Проследить подобное мы можем на примере США. Эти системы анализируют исторические данные об арестах для определения «горячих точек» преступности и направления туда полицейских патрулей. Однако, поскольку в прошлом полиция США непропорционально часто патрулировала районы проживания расовых меньшинств, данные об арестах уже являются предвзятыми. Алгоритм, обучаясь на них, неизбежно приходит к выводу, что именно эти районы являются наиболее опасными и наполненными криминалом, и рекомендует усилить там полицейское присутствие. Это создаёт самовоспроизводящийся «эффект обратной связи» (feedback loop). Усиленное патрулирование приводит к большему числу задержаний (часто за мелкие правонарушения), что, в свою очередь, генерирует новые данные, «подтверждающие» первоначальный предвзятый прогноз. В результате целые сообщества оказываются под постоянным и необоснованным давлением, что усиливает их стигматизацию и разрушает доверие к правоохранительным органам (и, по сути, усиливает криминал).

Скоринговые алгоритмы в финансах и рекрутинге. В этих сферах дискриминация часто носит более скрытый характер. Алгоритмы, оценивающие кредитоспособность или отбирающие кандидатов на работу, могут не использовать расу как прямой признак, но опираются на множество косвенных индикаторов (прокси), таких как почтовый индекс, уровень дохода района, тип оконченного учебного заведения или даже круг общения в социальных сетях. Все эти данные сильно коррелируют с расовой и этнической принадлежностью. Таким образом, происходит «цифровой редлайнинг» – практика, при которой система отказывает в услугах или предлагает менее выгодные условия представителям определённых групп, воспроизводя исторические паттерны сегрегации и экономического неравенства.

Анализ конкретных кейсов позволяет наглядно продемонстрировать масштабы проблемы и её социальные последствия. Как отмечают исследователи, изучение примеров из реальной жизни является «одним из лучших способов узнать об этических дилеммах» и сложностях, связанных с внедрением ИИ [6].

Одним из самых известных и широко обсуждаемых примеров является система COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), используемая в судебной

системе США для оценки вероятности рецидива у подсудимых. Расследование, проведённое в 2016 году изданием ProPublica, вскрыло глубокую расовую предвзятость этого алгоритма. Анализ показал, что COMPAS систематически завышал риски для афроамериканцев: они почти в два раза чаще, чем белые подсудимые с аналогичной криминальной историей, получали ложную метку «высокого риска» [5]. В то же время система чаще ошибалась в обратную сторону для белых обвиняемых, присваивая им незаслуженно низкий рейтинг риска. Защитники алгоритма утверждали, что он является «справедливым» по другому статистическому критерию (точности прогноза в целом), что положило начало сложной дискуссии о самом понятии «справедливости» в машинном обучении. Однако с точки зрения социального воздействия, система явно воспроизводила и усиливала стереотип об афроамериканцах как о более опасных преступниках, что могло влиять на решения судей о мере пресечения и приговорах.

Другой резонансный случай связан с технологией распознавания лиц Amazon Rekognition [8]. В 2018 году Американский союз защиты гражданских свобод (ACLU) провёл эксперимент, в ходе которого система сравнила фотографии всех членов Конгресса США с базой данных из 25 000 фотографий лиц, задержанных полицией. Результаты оказались шокирующими: Rekognition ошибочно идентифицировал 28 конгрессменов как преступников. Ошибки были непропорционально распределены: почти 40% из них пришлись на конгрессменов, принадлежащих к расовым меньшинствам, хотя они составляли лишь 20% от общего числа членов Конгресса. Этот эксперимент наглядно продемонстрировал опасность применения несовершенной технологии в правоохранительной сфере. Несмотря на шквал критики со стороны общественности и учёных, Amazon долгое время продолжала активно продавать технологию полиции. Лишь под давлением общественного мнения компания ввела временный мораторий на её использование правоохранительными органами.

Главной технической причиной расового уклона является недостаточная репрезентативность и качество данных. Тренировочные дата-сеты часто не отражают демографического разнообразия реального мира, что делает обученные на них модели менее точными для групп с меньшим количеством представителей. Однако проблема глубже, чем просто количество данных. Важен их контекст: кем, как и с какой целью они были собраны. Данные об арестах – это не объективные данные о преступности, а данные о деятельности полиции; и этот контекст часто игнорируется при создании моделей. Кроме того, существенную роль играет недостаток разнообразия в самой IT-индустрии. Команды разработчиков, в которых отсутствуют представители меньшинств, с большей вероятностью могут упустить из виду потенциальные риски предвзятости.

Последствия такой халатности выходят далеко за рамки технических неточностей – они ведут к усилению системного расового неравенства, созданию «цифровых гетто» и прямому нарушению прав человека. Внедрение дискриминирующих алгоритмов подрывает право на справедливое судебное разбирательство, презумпцию невиновности, право на частную жизнь и защиту от дискриминации. С этической точки зрения, попытка переложить ответственность на «нейтральный» алгоритм является опасным заблуждением. Как подчёркивают эксперты, ИИ не может считаться «искусственным моральным агентом», поскольку не обладает сознанием и субъектностью [1]. Таким образом, «ответственность за моральные риски разработки и внедрения» технологий и за сохранение «человеческого достоинства и прав человека в быстро меняющихся условиях» целиком и полностью лежит на людях (разработчиках, компаниях и государственных регуляторах). Без разработки чётких этических и правовых рамок, а также без внедрения обязательных механизмов прозрачности, аудита и подотчётности, технологии ИИ рискуют превратиться из инструмента прогресса в мощный механизм закрепления и легитимации вековой несправедливости.

Гендерный уклон демонстрирует, как ИИ активно формирует и усиливает социальные стереотипы о ролях мужчин и женщин, препятствуя достижению гендерного равенства. В отличие от расового уклона, который часто связан с недостатком данных, гендерный уклон чаще возникает из-за искаженного представления, повторяющего исторически сложившиеся культурные и институциональные барьеры.

Типичные проявления гендерной предвзятости охватывают профессиональную, лингвистическую и социальную сферы. Самый известный прецедент – система рекрутинга Amazon (2014-2017 гг.). Как сообщало агентство Reuters [8], ИИ-рекрутер был обучен на данных за предыдущее десятилетие, когда в IT-сфере доминировали мужчины. В результате система, приняв мужской паттерн за норму, автоматически понижала рейтинг резюме, содержащих слова, ассоциированные с женщинами (например, «женский колледж» или «председательница женского шахматного клуба») [8]. Это является классическим примером укоренения исторического институционального неравенства в алгоритме: технология создала цифровой барьер, основанный на прошлом успехе доминирующей группы.

Критический анализ этого кейса показывает, что алгоритм не был запрограммирован на сексизм, он был запрограммирован на поиск прокси-переменных, коррелирующих с успехом. В исторически несбалансированной выборке Amazon лучшей прокси-переменной для «успеха» оказался мужской пол. Таким образом, алгоритм не «ошибся», а математически точно воспроизвел институциональную предвзятость, заложенную в данных. Это иллюстрирует

фундаментальную проблему «оружия математического поражения» [10]: алгоритмы, оптимизированные для успеха, наказывают аутсайдеров и усиливают статус-кво.

Другое яркое проявление – стереотипизация в голосовых ассистентах. Большинство популярных помощников (Siri, Alexa) по умолчанию используют женские голоса. В отчете ЮНЕСКО «I'd Blush If I Could» («Я бы покраснела, если бы могла») [10] подчеркивается, что это усиливает и нормализует идею о том, что женщины должны быть «помощниками», всегда готовыми и доступными для выполнения команд. Критика ЮНЕСКО сосредоточена не только на голосе, но и на алгоритмах ответа: в ответ на оскорбления или домогательства ассистенты запрограммированы отвечать пассивно или кокетливо. Как отмечают в «ООН-женщины» (UN Women) [9], такое проектирование закрепляет патриархальные установки и недооценивает женский авторитет в технологической сфере.

Этот уклон также глубоко укоренен в языковых моделях. Модели, обученные на огромных массивах текстов (исторических книг, новостных архивов), наследуют лингвистические гендерные стереотипы. Примером выступают векторные аналогии: (Король – Мужчина) + Женщина = Королева. Но тот же принцип приводит к аналогии (Врач – Мужчина) + Женщина = Медсестра. Это лингвистическое укоренение стереотипов, которое Сафия Ноубл назвала «алгоритмами угнетения» [6, стр. 64], влияет на перевод, поиск информации (где запросы о «профессиях для женщин» выдают низкооплачиваемые позиции) и, как следствие, на восприятие профессиональных возможностей.

Наиболее остро проблема проявляется в интерсекциональном уклоне. Исследование «Gender Shades» показало, что коммерческие системы определения пола от ведущих ИТ-корпораций демонстрируют наивысший уровень ошибок именно для темнокожих женщин (до 34.7% ошибок) [5, стр. 80]. В то же время, для белых мужчин ошибка не превышала 0.8%. Это доказывает, что технологический «обычный» человек – белый мужчина, а системы не тестируются на уязвимых группах. Это пересечение гендерного и расового уклонов, основанное на нерепрезентативности данных в обеих категориях [2, стр. 1250].

Причины возникновения гендерного уклона сложны и многогранны. Во-первых, это неравенство в STEM и IT-отраслях. Значительный гендерный дисбаланс в IT приводит к тому, что дизайн и этические рамки ИИ часто формируются однородным составом разработчиков. Во-вторых, это репликация социальных ролей: алгоритмы, обученные на исторических данных, воспринимают исторически сложившиеся социальные роли как статистическую норму для прогнозирования.

Этические последствия и общественная реакция на гендерный уклон глубоки. Укорененный уклон ограничивает социальную мобильность и закрепляет стереотипы. В ответ на

это возникло научное направление феминистской этики технологий, требующее пересмотра самой парадигмы разработки ИИ и внедрения инклюзивных принципов. На институциональном уровне это привело к созданию международных и национальных инициатив, таких как российский Кодекс этики в сфере ИИ, который включает принципы справедливости и недискриминации.

После всестороннего анализа проблемы укоренения дискриминации критически важно перейти к поиску эффективных путей ее преодоления на всех уровнях: от технического до социального.

Преодоление укорененной социальной дискриминации в алгоритмах ИИ требует комплексного, междисциплинарного подхода, который сочетает техническую коррекцию моделей с этическим регулированием и социальными изменениями. Убеждение, что проблему можно решить чисто техническими методами (техно-солюционизм), является ошибочным, поскольку игнорирует социальные корни проблемы.

Технические меры направлены на устранение предвзятости на уровне данных и алгоритмов. Важнейшим шагом является алгоритмический аудит и тестирование на предвзятость. Это не разовая процедура, а постоянный процесс мониторинга. Как отмечают исследователи ВШЭ, аудит должен включать тестирование на дискриминационный эффект, то есть, оценку того, оказывает ли алгоритм несправедливое воздействие на уязвимые группы, даже если он не использует прямые маркеры расы или гендера [1, стр. 67]. Однако техническая предвзятость сама по себе является этической проблемой: «очищая» данные от исторической предвзятости (например, искусственно выравнивая количество успешных резюме от мужчин и женщин в кейсе Amazon), мы рискуем снизить прогностическую точность модели или создать новую, искусственную реальность.

Более сложной задачей является выбор метрик справедливости. Как убедительно показывают Барокас и Зельбст, часто существует математический компромисс между различными определениями справедливости [6]. Например, «групповая справедливость» (обеспечение равного процента положительных решений для мужчин и женщин) может противоречить «индивидуальной справедливости» (гарантия, что похожие индивидуумы получат похожие решения). Выбор между этими метриками является не техническим, а этико-политическим решением, которое разработчики часто принимают скрыто. Развитие «Объяснимого ИИ» (Explainable AI (XAI)) также не является панацеей. Прозрачность не гарантирует справедливости. Знание того, что вам отказали в кредите из-за вашего почтового индекса (прокси-расы), не отменяет дискриминационного исхода.

Поскольку технические меры ограничены, они должны подкрепляться этическими и институциональными мерами. На этом уровне происходит переход от «мягкого права» к «жесткому праву». Большинство существующих рамок, включая Рекомендации ЮНЕСКО и российский Кодекс этики в сфере ИИ, носят декларативный, добровольный характер. Они повышают осведомленность, но не имеют механизмов принуждения. В противовес этому, Европейский Союз разработал Регламент по ИИ (AI Act), в нем центральный подход основан на категоризации рисков. Системы ИИ (например, в правосудии или рекрутинге) признаются «высокорисковыми» и подлежат обязательной внешней сертификации и оценке воздействия на права человека, как к тому призывает Управление Верховного комиссара ООН по правам человека Российская правовая мысль также активно разрабатывает подходы к регулированию, однако основной вызов заключается в адаптации существующего права к автономным системам, принимающим решения.

Наконец, наиболее фундаментальным уровнем являются образовательные и социальные меры, поскольку невозможно создать «справедливый» ИИ в несправедливом обществе. Долгосрочным решением является привлечение женщин и меньшинств в разработку ИИ. Увеличение разнообразия в командах разработчиков – это не символический жест, а практическая необходимость. Как доказывает кейс Gender Shades, разнообразные команды (включающие темнокожих женщин) с большей вероятностью заметят «слепые зоны» в данных и протестируют систему на уязвимых группах до ее внедрения. В краткосрочной перспективе, как отмечает В. Лепский [3], необходимо внедрение междисциплинарных команд, где инженеры работают в связке с этиками, социологами и историками. Только гуманитарий может провести исторический аудит данных и оценить социальный контекст, который алгоритм неспособен «увидеть».

Успешное преодоление алгоритмической дискриминации требует слияния технических инноваций с гуманитарным осмыслением, что подтверждает необходимость междисциплинарного подхода.

Заключение. Проведённый анализ убедительно подтверждает, что ИИ не является нейтральной технологией, а выступает мощным механизмом, закрепляющим исторически сложившиеся предубеждения общества. Расовый уклон, проявляющийся в прогностической полиции, и гендерный уклон, закрепляющий стереотипы в рекрутинге, создают прямую угрозу фундаментальным правам и свободам, особенно на уровне интерсекционального уклона. Главной причиной этого является недостаточная репрезентативность и качество данных. Преодоление алгоритмической дискриминации требует комплексной стратегии, выходящей за рамки технического решения. Она включает обязательный и постоянный алгоритмический

аудит, переход от добровольных кодексов этики к «жёсткому праву», требующему обязательной сертификации систем высокого риска, а также увеличение разнообразия в командах разработчиков.

Список источников и литературы:

1. Игнатьев А. Г. Этика и проблемы искусственного интеллекта / А. Г. Игнатьев. – Текст : электронный // М.: НИУ «Высшая школа экономики», 2024. – Т. 24, № 1. – С. 87-100. – URL: https://publications.hse.ru/pubs/share/direct/959145000.pdf. (дата обращения: 05.11.2025);
2. Кодекс этики в сфере искусственного интеллекта [Электронный ресурс] / Альянс в сфере ИИ. – М., 2021. – Режим доступа: https://ethics.a-ai.ru/ (дата обращения: 05.11.2025);
3. Лепский В. Е. Искусственный интеллект в субъектных парадигмах управления / В. Е. Лепский. – Текст : электронный // Философские науки. – 2021. – Т. 64, № 1. – С. 88–101. – URL: https://www.phisci.info/jour/article/view/3329/3085 (дата обращения: 05.11.2025);
4. Луценко А. «Amazon объявила о сокращении 14 тыс. сотрудников ради внедрения ИИ» / А. Луценко. – М.: РБК, 2025. – URL: https://www.rbc.ru/rbcfreenews/6900d1969a7947bc30f35f4e. – Текст : электронный (дата обращения: 05.11.2025);
5. Понкин И. В. Искусственный интеллект и правовая дискриминация / И. В. Понкин, А. И. Редькина. – Текст : электронный // Государство и право. – 2020. – № 10. – С. 66–75. – URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-pravovaya-diskriminatsiya (дата обращения: 05.11.2025);
6. Шталь Б. К. Этика искусственного интеллекта : кейсы и варианты решения этических проблем / Б. К. Шталь, Д. Шредер, Р. Родригес / Текст : электронный. – М.: Изд-во Института Гайдара, 2024. – URL: https://cyberleninka.ru/article/n/etika-iskusstvennogo-intellekta-keysy-i-varianty-resheniya-eticheskih-problem (дата обращения: 05.11.2025);
7. Buolamwini J. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification / J. Buolamwini, T. Gebru. – Text : electronic // Proceedings of the 1st Conference on Fairness, Accountability and Transparency. – 2018. – P. 77-91. – URL: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (date of acces: 05.11.2025);
8. Dastin J. Amazon scraps secret AI recruiting tool that showed bias against women [Electronic sourse] / J. Dastin // Reuters. – 2018. – URL: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ (date of acces: 05.11.2025);
9. Del Villar Z. How AI reinforces gender bias – and what we can do about it [Electronic sourse] / Z. Del Villar. – Text : electronic. – New York: UN Women. – 2025. – URL: https://www.unwomen.org/en/news-stories/interview/2025/02/how-ai-reinforces-gender-bias-and-what-we-can-do-about-it (date of acces: 05.11.2025);
10. West M. I'd Blush If I Could: closing gender divides in digital skills through education [Electronic sourse] / M. West, R. Kraut, H. Ei Chew [et al.]. – Text : electronic. – Paris: UNESCO, EQUALS Skills Coalition, 2019. – 132 p. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000367416 (date of access: 05.11.2025).

Артем Алексеевич Олифиренко,
AICP-E, GDPR-DPP, специалист по защите данных, ответственный за безопасность систем искусственного интеллекта
ООО «Экосистема недвижимости «Метр квадратный» (ВТБ-группа),
магистрант Института магистратуры и заочного обучения Саратовской государственной юридической академии,
магистрант Института электронной техники и приборостроения Саратовского государственного технического университета им. Гагарина Ю. А.,
E-mail: artemolifirenko@yandex.ru

Artem A. Olifirenko,
AICP-E, GDPR-DPP, Data Protection Specialist and AI Security Lead,
Metr Kvadratny Real Estate Ecosystem LLC (VTB Group),
Master's student, Institute of Magistracy and Distance Learning, Saratov State Law Academy,
Master's student, Institute of Electronic Engineering and Instrumentation, Yuri Gagarin Saratov State Technical University,
E-mail: artemolifirenko@yandex.ru

УПРАВЛЕНИЕ РИСКАМИ ОБУЧЕНИЯ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТРАНСГРАНИЧНОЙ СРЕДЕ

RISK MANAGEMENT IN CROSS-BORDER TRAINING OF ARTIFICIAL INTELLIGENCE MODELS

Аннотация. В статье рассматриваются ключевые правовые и технические риски, возникающие при обучении моделей искусственного интеллекта в трансграничной среде. Анализируются требования Регламента (ЕС) 2024/1689 («Закон об ИИ») и Общего регламента по защите данных (Регламент 2016/679), определяющие правила происхождения данных, их международной передачи и дальнейшего использования. Обосновывается необходимость комплексной системы управления рисками, включающей прослеживаемость источников данных и применение защитных технологий.

Abstract. This article examines the key legal and technical risks that arise when training artificial intelligence models in a cross-border environment. It analyses the requirements of Regulation (EU) 2024/1689 («AI Act») and the General Data Protection Regulation (Regulation (EU) 2016/679), which establish rules governing data provenance, international data transfers, and subsequent use. The article substantiates the need for an integrated risk management framework, including end-to-end traceability of data sources and the deployment of protective technologies.

Ключевые слова: искусственный интеллект, трансграничные данные, AI Act, GDPR, обучение моделей, риски, происхождение данных.

Keywords: artificial intelligence, cross-border data, AI Act, GDPR, model training, risks, data provenance.

Развитие трансграничного регулирования обучения моделей искусственного интеллекта (ИИ-модели) требует чёткого понимания нормативной базы, определяющей обязанности разработчиков, поставщиков и операторов. Центральное место в архитектуре европейского правового регулирования занимает Регламент ЕС 2024/1689 (Закон об ИИ) [6], который устанавливает дифференцированные требования к различным видам ИИ-моделей, включая модели общего назначения (МОН). Для таких моделей введена обязанность публиковать «сводку содержания» обучающих данных, отражённую в ст. 53(1)(d) Закона об ИИ. Эта сводка должна описывать основные категории источников, используемых в обучении, и обеспечивать минимальный уровень прозрачности относительно происхождения данных. Правовой режим МОН дополняется Кодексом надлежащей практики, разработанным в рамках европейской инициативы по саморегулированию индустрии [1]. Положения данного кодекса конкретизируют способы выполнения требований Закона об ИИ: разделы, посвящённые прозрачности и авторскому праву, направлены на реализацию ст. 53 Закона об ИИ, а разделы о безопасности, тестировании и управлении рисками – на исполнение ст. 55, включая оценку системных рисков, методы предотвращения вреда и механизмы внутреннего контроля.

Существенное значение имеет вопрос происхождения данных, использованных при обучении моделей, а также оценка их качества, законности и надлежащего получения [3]. Если в составе обучающих выборок присутствуют персональные данные, к ним подлежат применению принципы Общего регламента по защите данных (Регламент 2016/679), закреплённые в ст. 5: законность, добросовестность и прозрачность; ограничение цели обработки; минимизация объёма; точность данных; ограничение хранения; обеспечение целостности и конфиденциальности; а также ответственность оператора за соблюдение всех принципов. Нечёткая структура источников, отсутствие документированного происхождения данных или возможное включение нелегитимно собранных массивов создаёт риск нарушения принципов минимизации и ограниченности цели [2].

По нормам Регламента 2016/679 трансграничная передача персональных данных допускается лишь при соблюдении жёстких условий, установленных в ст. 44-50. Базовый принцип ст. 44 закрепляет, что передача возможна только при условии, что совокупность применяемых мер обеспечивает отсутствие подрыва уровня защиты, гарантированного внутри ЕС. На практике допустимы три механизма: признание страной назначения «адекватного уровня» защиты (ст. 45), применение «надлежащих гарантий» в форме стандартных договорных

условий или внутренних корпоративных правил (ст. 46), а также узкие и ограниченные исключения (ст. 49), включая явное согласие субъекта данных, необходимость исполнения договора или соображения существенного общественного интереса. Передача данных в юрисдикции, не обладающие статусом адекватности, требует проведения детальной оценки средств защиты, включая возможность технической псевдонимизации, распределённого хранения или шифрования, а также заключения дополнительных соглашений, компенсирующих недостатки национального законодательства.

Закон об ИИ содержит специальные нормы, обязывающие поставщиков, не имеющих представительства в ЕС, назначать авторизованного представителя, который несёт ответственность за выполнение требований Регламента 2016/679 и взаимодействие с надзорными органами (ст. 21). При закупке моделей общего назначения или наборов данных за пределами ЕС необходима комплексная юридическая проверка (оценка должной осмотрительности), охватывающая законность получения данных, соблюдение авторских прав, риски включения персональных данных без надлежащего правового основания, а также возможное наличие запрещённых категорий данных [5]. Существенное значение имеет и экспортный контроль: в зависимости от страны происхождения модель может подпадать под ограничения на передачу технологий двойного назначения, что требует проверки применимых регуляторных условий и санкционных списков Европейского Союза, США, Великобритании и иных юрисдикций. Несоблюдение указанных требований может привести к нарушению запретов на экспорт технологий либо к косвенной передаче запрещённых алгоритмов, что влечёт юридическую ответственность для европейских участников цепочки поставок [4].

Заключение. Так, проведённый в рамках научной работы анализ показал, что ключевым элементом системы обеспечения соответствия требованиям является законность и прозрачность происхождения данных, используемых для обучения. Невозможность подтвердить источники, соблюдение условий сбора или правомерность трансграничной передачи данных приводит к автоматическому возникновению рисков нарушения Регламента 2016/679 и запрета на дальнейшее использование набора данных для обучения, независимо от технической сложности модели. В условиях глобальных цепочек поставок ИИ именно этот аспект формирует наибольшую уязвимость разработчиков.

Список источников и литературы:

1. EU AI Act: General Purpose AI. Code of Practice. Final Version – 10.07.2025 [Электронный ресурс]. URL: https://code-of-practice.ai/?section=summary (дата обращения: 08.11.2025).

2. Hohmann B., Kollár G. Reflections on the data protection compliance of AI systems under the EU AI Act [Электронный ресурс] // Cogent Social Sciences. – 2025. – Vol. 11, No. 1. – URL: https://doi.org/10.1080/23311886.2025.2560654 (дата обращения: 08.11.2025).

3. Holtz H.M., Ledendal J. AI Data Governance – Overlaps Between the AI Act and the GDPR. Forthcoming in Law, Innovation and Technology [Электронный ресурс]. URL: https://uu.diva-portal.org/smash/get/diva2:1996843/FULLTEXT01.pdf (дата обращения: 08.11.2025).

4. Jørgensen B.N., Ma Z.G. Impact of EU Regulations on AI Adoption in Smart City Solutions: A Review of Regulatory Barriers, Technological Challenges, and Societal Benefits [Электронный ресурс] // Information. – 2025. – Vol. 16, No. 7. – URL: https://doi.org/10.3390/info16070568 (дата обращения: 08.11.2025).

5. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models [Электронный ресурс] // European Data Protection Board. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en (дата обращения: 08.11.2025).

6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008, (EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1 // OJ L, 2024/1689, 12.7.2024.

Алексей Вячеславович Ордин,
докторант Московского авиационного института (государственного технического университета),
магистр международных отношений,
магистр права, к.т.н., эксперт в области цифровой дипломатии и международной кибербезопасности,
E-mail: Alexey_ordin@mail.ru

Alexey V. Ordin,
Doctoral Candidate, Moscow Aviation Institute (National Research University),
Master of International Relations,
Master of Law, Ph.D. in Engineering, expert in digital diplomacy and international cybersecurity,
E-mail: Alexey_ordin@mail.ru

РОССИЯ И АРМЕНИЯ В ЦИФРОВУЮ ЭПОХУ: КИБЕРБЕЗОПАСНОСТЬ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК НОВЫЕ ИЗМЕРЕНИЯ МЕЖДУНАРОДНОЙ ПОЛИТИКИ

RUSSIA AND ARMENIA IN THE DIGITAL AGE: CYBERSECURITY AND ARTIFICIAL INTELLIGENCE AS NEW DIMENSIONS OF INTERNATIONAL POLITICS

Аннотация. В статье рассматриваются нормативно-правовые и институциональные аспекты кибербезопасности в Республике Армения, ее международная позиция в сфере информационной безопасности и искусственного интеллекта, а также точки соприкосновения и потенциального сотрудничества с Российской Федерацией. На основе анализа недавно принятых законов, участия Армении в резолюциях ООН и международных инициатив рассматривается влияние этих процессов на цифровой суверенитет, международные отношения и трансформацию мировой политики. Особое внимание уделено количественной оценке критической информационной инфраструктуры (КИИ) и перспективам финансирования киберзащиты.

Ключевые слова: кибербезопасность, цифровой суверенитет, искусственный интеллект, международная политика.

Abstract. This article examines the regulatory and institutional aspects of cybersecurity in the Republic of Armenia, its international position in the fields of information security and artificial intelligence, as well as points of convergence and potential cooperation with the Russian Federation. Based on the analysis of recently adopted laws, Armenia's participation in UN resolutions, and international initiatives, the study explores the impact of these processes on digital sovereignty, international relations, and the transformation of global politics. Special attention is given to the quantitative assessment of critical information infrastructure (CII) and prospects for cybersecurity funding.

Key words: cybersecurity, digital sovereignty, artificial intelligence, international politics.

Введение. Киберпространство и технологии искусственного интеллекта стали ключевыми факторами формирования международной безопасности и устойчивости государств. Россия и Армения, обладая тесными стратегическими связями, активно формируют нормативную и институциональную базу для обеспечения цифрового суверенитета, защиты критической инфраструктуры и этичного применения ИИ. Принятие в Армении закона «О кибербезопасности» и участие в международных дебатах подтверждают возрастающую значимость этих вопросов для национальной и региональной политики [1, 2].

Национальная киберполитика Армении. В 2025 году Правительство Армении утвердило пакет законопроектов, включая закон «О кибербезопасности», закон «Об общественной информации» и закон «О регулирующем органе информационных систем». Закон «О кибербезопасности» формализует систему предотвращения и реагирования на киберинциденты, устанавливает полномочия государственных органов и предусматривает координацию с частным сектором [1]. Публичные обсуждения законопроекта с марта 2025 года позволили учитывать мнение бизнеса, экспертов и международных партнеров, формируя прозрачный и инклюзивный процесс законодательной подготовки.

Оценка критической информационной инфраструктуры. По предварительным оценкам экспертов, в Армении насчитывается около 50–200 объектов КИИ, включая энергетические системы, водоснабжение, телекоммуникации, государственные информационные системы, транспортные коммуникации, финансовые учреждения и дата-центры [2, 3]. Предстоящая цифровизация и создание крупных центров обработки данных в Республике Армения увеличивают нагрузку на защиту КИИ и требуют модернизации национальной системы кибербезопасности.

Перспективы бюджета Армении на киберзащиту. Ориентировочный рост бюджетных расходов на кибербезопасность в Республике Армения в ближайшие годы обусловлен как модернизацией критической информационной инфраструктуры (КИИ), так и развитием национальных центров реагирования на киберинциденты. По предварительным оценкам экспертов [2], при текущих потребностях в защите государственных информационных систем, финансовых и энергетических объектов ежегодные расходы могут составить примерно 15-45 млн USD. Эти средства предполагается направить на закупку современного оборудования межсетевого экранирования, систем мониторинга, средств обнаружения вторжений, а также на подготовку квалифицированных кадров в области кибербезопасности.

При активной цифровизации экономики, внедрении электронного правительства, расширении числа объектов КИИ и интеграции с международными платформами киберзащиты расходы могут вырасти до 70-150 млн USD в год. В этом случае бюджет будет включать

финансирование не только инфраструктуры, но и программного обеспечения, платформ анализа данных, систем искусственного интеллекта для предотвращения киберинцидентов, а также международного сотрудничества в рамках обмена информацией и проведения совместных учений по киберзащите. Оценки также учитывают потребность в резервировании средств на экстренные реагирования при крупных инцидентах, включая атаки на энергетические и финансовые объекты, транспортные сети и телекоммуникации, что особенно актуально для Армении как транзитного цифрового узла в регионе [3].

Международная позиция Армении. Армения активно участвует в глобальном кибердиалоге и укрепляет свои позиции как государство, заинтересованное в формировании международных стандартов безопасного использования ИКТ. В 2024 и 2025 годах страна поддержала ряд резолюций Генеральной Ассамблеи ООН, инициированных Российской Федерацией, посвященных роли ООН в разработке правил ответственного поведения государств в киберпространстве [4].

Такая поддержка отражает стратегический выбор Армении, направленный на укрепление цифрового суверенитета, соблюдение норм международного права и предотвращение милитаризации информационного пространства. При этом Армения сохраняет баланс между национальными интересами и международными обязательствами, активно взаимодействуя с партнерами по вопросам киберустойчивости, обмена данными о киберинцидентах и координации совместных учений. Поддержка резолюций на уровне ООН также позволяет Армении участвовать в разработке механизмов международной сертификации и оценки киберустойчивости, что повышает доверие к национальным системам и открывает доступ к передовым технологическим решениям [4].

Ханойская Конвенция о киберпреступности. 25 октября 2025 года в Ханое, Вьетнам, официально открылась для подписания Конвенция Организации Объединенных Наций против киберпреступности [5]. Этот международный инструмент призван унифицировать подходы к противодействию киберпреступлениям, включая уголовное преследование киберпреступников, международное сотрудничество в расследованиях и обмен доказательной базой.

Армения пока не подписала Конвенцию, что обусловлено прагматичной стратегией постепенной интеграции в международные механизмы регулирования. Основная причина заключается в желании сначала оценить эффективность недавно принятого национального законодательства «О кибербезопасности», отработать работу созданных структур защиты КИИ и убедиться в их готовности к международной интеграции [2]. Такой подход позволяет минимизировать риски, связанные с возможными несоответствиями национального регулирования международным требованиям, а также проверить способность государственных

и частных операторов реагировать на сложные киберинциденты и координировать свои действия на трансграничном уровне.

Кроме того, временная пауза в подписании Конвенции дает Армении возможность выстроить систему подготовки специалистов, разработать методики оценки уязвимостей критической инфраструктуры и протестировать механизмы обмена информацией с международными партнерами, чтобы присоединение к соглашению было максимально безопасным и эффективным. Ожидается, что после завершения первых этапов реализации национальной стратегии кибербезопасности и подтверждения ее эффективности, Армения рассмотрит возможность подписания Ханойской Конвенции, что позволит стране закрепить свои позиции в международных структурах кибербезопасности и повысить доверие к национальной инфраструктуре на глобальном уровне [5].

Институциональное развитие. Национальная команда реагирования на компьютерные инциденты AM-CERT, аккредитованная в международной ассоциации TF-CSIRT с января 2024 года, обеспечивает обмен информацией о киберинцидентах и интеграцию в глобальные практики реагирования [6].

Информационное агентство систем Армении (ISAA) является ключевым оператором национальной кибербезопасности, отвечающим за мониторинг, защиту и реагирование на инциденты.

Искусственный интеллект: этика и право. Армения намерена подписать Рамочную конвенцию Совета Европы об искусственном интеллекте, правах человека и верховенстве права. 25 сентября 2025 года заместитель министра иностранных дел Республики Армения выступил на заседании Совета Безопасности ООН «Искусственный интеллект и международный мир и безопасность» [6], подчеркнув необходимость применения международного гуманитарного права к автономным системам и соблюдения принципов законности, пропорциональности и различения [7]. Россия придерживается схожих подходов: Национальная стратегия развития искусственного интеллекта, утверждённая в 2023 году, акцентирует внимание на обеспечении безопасности алгоритмов, этичности их применения и формировании международных норм в сфере ИИ [7].

Россия и Армения: сотрудничество и сопоставление стратегий. Обе страны признают цифровой суверенитет ключевым принципом, выступают за межгосударственное регулирование ИКТ и этичные стандарты ИИ. Совместная работа может включать:

1. обмен данными о киберинцидентах;
2. подготовку кадров;
3. реализацию исследовательских проектов;

4. гармонизацию стандартов киберустойчивости;

5. разработку доверенных цифровых сервисов [6, 7].

Заключение. Принятие Арменией закона «О кибербезопасности» и активное участие страны в международных дискуссиях по вопросам информационной безопасности и искусственного интеллекта демонстрируют значительный сдвиг от фрагментарного регулирования к системной и стратегически выстроенной национальной киберполитике. Новый закон формализует систему предотвращения и реагирования на киберинциденты, задает правовую основу для взаимодействия государственных органов и частного сектора, а также создает предпосылки для прозрачного и предсказуемого функционирования критической информационной инфраструктуры (КИИ). Такой подход укрепляет доверие к государственным и корпоративным информационным системам, снижает риски кибератак и создает условия для устойчивого развития цифровой экономики страны. Комплиментарность подходов России и Армении укрепляет стратегическое партнерство и способствует формированию безопасной и предсказуемой цифровой архитектуры будущего на региональном и глобальном уровне.

Список источников и литературы:

1. Закон Республики Армения «О кибербезопасности» (2025) // Национальное законодательство Республики Армения.

2. В Армении создадут комиссию по кибербезопасности критических объектов [Электронный ресурс] // Sputnik Армения. 21.11.2025. URL: https://am.sputniknews.ru/20251121/v-armenii-sozdadut-komissiyu-po-kiberbezopasnosti-kriticheskikh-obektov-96083814.html (дата обращения: 08.12.2025).

3. Национальная команда реагирования на компьютерные инциденты AM-CERT. Отчет за 2025 год [Электронный ресурс] // AM-CERT. URL: https://www.amcert.am/reports/2025 (дата обращения: 08.12.2025).

4. Национальная стратегия Российской Федерации в области искусственного интеллекта (2023) [Электронный ресурс] // Министерство цифрового развития Российской Федерации. URL: https://digital.gov.ru/ru/activity/strategy/ai/ (дата обращения: 08.12.2025).

5. Участие Армении в резолюциях Генеральной Ассамблеи ООН по кибербезопасности (2024–2025) [Электронный ресурс] // UN Digital Cooperation. URL: https://www.un.org/en/ga/cybersecurity-resolutions (дата обращения: 08.12.2025).

6. Armenia: Digital Connectivity - Leaving No One Behind [Electronic resource] // Eurasian Development Bank (EDB). 15.07.2025. URL: https://www.eabr.org/en/projects/digital-connectivity-armenia/ (дата обращения: 08.12.2025).

7. Global Cybersecurity Capacity Building Report 2024 [Electronic resource] // United Nations Open-Ended Working Group on ICT Security. URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2024/09/oewg-capacity-report.pdf (дата обращения: 08.12.2025).

8. United Nations Convention against Cybercrime (Hanoi Convention) (25.10.2025) [Electronic resource] // United Nations Office on Drugs and Crime (UNODC). URL: https://www.unodc.org/unodc/en/cybercrime/hanoi-convention.html (дата обращения: 08.12.2025).

Евгения Михайловна Рогожина,
к.п.н., доцент кафедры международных отношений
и зарубежного регионоведения,
ФГБОУ ВО «Нижегородский государственный
лингвистический университет имени Н. А. Добролюбова»
E-mail: evgenia-amiga@yandex.ru

Александр Дмитриевич Кузнецов,
Высшая школы международных отношений и мировой политики,
ФГБОУ ВО «Нижегородский государственный
лингвистический университет имени Н. А. Добролюбова»,
E-mail: Kuznetsov.200@yandex.ru

Evgeniya M. Rogozhina,
PhD in Political Science,
Associate Professor,
Department of International Relations and Regional Studies,
Linguistic University of Nizhny Novgorod
E-mail: evgenia-amiga@yandex.ru

Alexander D. Kuznetsov,
Higher School of International Relations and World Politics,
Linguistic University of Nizhny Novgorod,
E-mail: Kuznetsov.200@yandex.ru

РЕАЛИЗАЦИЯ ИНИЦИАТИВ В ОБЛАСТИ МЕЖДУНАРОДНОГО УПРАВЛЕНИЯ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

IMPLEMENTATION OF INITIATIVES IN THE FIELD OF INTERNATIONAL ARTIFICIAL INTELLIGENCE MANAGEMENT

Аннотация. В 2020-е годы мир подошёл к развилке: искусственный интеллект перестал быть лишь предметом футурологических прогнозов и превратился в элемент повседневности, влияющий на экономику, безопасность и права человека. В этих условиях международные организации постепенно отходят от общих деклараций и начинают выстраивать устойчивые институты управления. В данной статье рассматривается, как складывается система регулирования на уровне Организации Объединённых Наций, БРИКС и Шанхайской организации сотрудничества. В рамках ООН анонсированы Независимая международная научная панель и Глобальный диалог по ИИ, которые должны обеспечить экспертное сопровождение и площадку для обсуждения без доминирования отдельных стран. БРИКС, объявив о стремлении выработать правила для искусственного интеллекта, уже запускает совместные исследовательские группы и открывает центры развития и сотрудничества. ОС делает ставку на региональный аспект и планирует создание Центральноазиатского центра ИИ, обеспечивающего доступ к технологиям и кадрам для стран Центральной Азии. В статье анализируются препятствия на пути этих инициатив: глубокий цифровой разрыв, противоречия между национальным суверенитетом и многосторонним подходом, консультационный характер принятых решений и дефицит ресурсов.

Ключевые слова: искусственный интеллект, международное регулирование ИИ, ООН, БРИКС, ШОС, управление ИИ.

Abstract. In the 2020s artificial intelligence (AI) moved from a futuristic concept to a daily reality, affecting economies, security and human rights. In response, international organisations are shifting from general declarations to the creation of lasting governance structures. This article examines how the United Nations, BRICS and the Shanghai Cooperation Organisation build their regulatory frameworks. Within the UN, an Independent International Scientific Panel and a Global Dialogue on AI have been announced to provide expert guidance and an inclusive forum free from the dominance of individual states. BRICS, having declared a commitment to global AI governance, is already launching joint study groups and opening centres for AI development and cooperation. The SCO focuses on the regional dimension, planning a Central Asian AI centre to provide technology and human capital to the region. The paper also discusses obstacles to these initiatives: the deep digital divide, tensions between national sovereignty and multilateralism, the advisory nature of the proposed mechanisms, and the scarcity of resources.

Key words: artificial intelligence, international regulation of AI, the United Nations, BRICS, the SCO, AI governance.

За последнее десятилетие искусственный интеллект превратился из технологии узкого применения в фактор, определяющий будущее общества. Алгоритмы машинного обучения используются в промышленности и транспорте, медицине и образовании, помогают выявлять преступления и оптимизировать энергопотребление. Но вместе с ростом возможностей увеличиваются и риски: от усиления социального неравенства до появления автономного оружия. В разных странах обсуждение ИИ-регулирования долгое время сводилось к кодексам принципов и этическим декларациям. Однако к середине 2020-х стало понятно, что без институциональной базы этот подход не сработает, поскольку необходимо экспертное сопровождение, площадки для переговоров и механизмы финансирования.

Реализация инициатив ООН. Организация Объединённых Наций первой предложила перейти от общих принципов к конкретным механизмам. В конце 2023 года Генеральный секретарь объявил о намерении создать Независимую международную научную группу (панель)

по ИИ и запустить Глобальный диалог по вопросам управления ИИ. Важно, что в конце 2025 года Генеральная Ассамблея приняла резолюцию A/RES/79/325, в которой закрепила мандат и формат работы обоих механизмов [1, с. 1-4; 2; 7]. Что касается панели, она представляет из себя научную группу, которая должна готовить ежегодные доказательные оценки о возможностях, рисках и эффектах использования ИИ, а также должна выпускать тематические материалы. Материалы должны служить источником объективной базы для обсуждений и переговоров государств.[1, с.1-2, 4; 2] В дополнение к этому ООН учреждает Глобальный диалог по вопросам управления ИИ как регулярно созываемую для всех заинтересованных акторов площадку, ориентированную на открытость и инклюзивность, обмен практиками и обсуждение сотрудничества для сокращения цифрового разрыва [1, с.2-4; 5].

Пока что эти структуры носят консультативный характер: рекомендации не являются обязательными, а бюджет инициатив ограничен. Тем не менее, это важный шаг от разрозненных деклараций к формированию глобальной архитектуры. ООН фактически взяла на себя роль координатора, который сводит участников, обобщает опыт и предлагает стандарты, но без жестких ограничений. Вызов в том, чтобы вовлечь страны Глобального Юга, для которых ИИ может стать не только возможностью, но и источником новых зависимостей из-за цифрового разрыва.

Реализация инициатив БРИКС. Группа БРИКС уже давно рассматривается Россией как одна из опор «поворота на Восток». В отличие от ООН, где доминируют универсальные механизмы, БРИКС строит свои проекты вокруг идеи цифрового суверенитета и определенного сотрудничества. На саммите 2025 года лидеры стран группы приняли заявление о глобальном управлении искусственным интеллектом, подчеркнув необходимость уважать национальные особенности и право каждого государства контролировать свои данные [3]. Заявления и декларации достаточно быстро подкрепили конкретикой. В сентябре 2025 года в Сямэне прошла конференция, организованная Организацией Объединённых Наций по промышленному развитию. В рамках мероприятия была запущена совместная лаборатория «Китай – БРИКС» и открыты Центр развития и сотрудничества в области искусственного интеллекта и Платформа инноваций БРИКС. Параллельно представили фонд доверия для поддержки проектов ИИ в развивающихся странах и «зелёный индекс AIM» для оценки экологической устойчивости алгоритмов [4]. Всё это говорит о том, что БРИКС переходит к практике, т. е. формируются исследовательские группы, создаются базы данных и образовательные программы, обеспечивается финансирование. Принципиальным для БРИКС остаётся баланс между инклюзивностью и защитой суверенитета. С одной стороны, участники стремятся обмениваться технологиями и совместно разрабатывать стандарты, чтобы не зависеть от западных компаний.

С другой – каждая страна хочет сохранить контроль над данными, что затрудняет создание единого регуляторного поля. Российская дипломатия в этом диалоге играет заметную роль: Москва предлагает продвигать идеи цифрового суверенитета, одновременно укрепляя связи со странами Востока.

Реализация инициатив ШОС. Для стран Шанхайской организации сотрудничества искусственный интеллект – ещё один инструмент укрепления взаимосвязей в Евразии. На Тяньцзиньском саммите, прошедшем 31 августа –1 сентября 2025 года, участники поддержали планы открыть Центральноазиатский центр искусственного интеллекта в Душанбе и разработать специальный механизм сотрудничества в этой области [6, с.4]. В декларации подчёркивается, что технологии должны быть доступны всем государствам, а не становиться рычагом давления. Региональный центр предполагается использовать для координации исследований, обмена практиками и подготовки кадров, чтобы сократить разрыв между государствами-лидерами и остальными странами. Инициатива ШОС логично дополняет глобальные проекты ООН и БРИКС, предлагая региональную экспертизу. Вместе с тем остаётся открытым вопрос финансирования: создание инфраструктуры и поддержка обучения требуют значительных ресурсов. Важно также предусмотреть механизмы кибербезопасности и защиты данных, чтобы совместные проекты не стали источником уязвимостей.

Проблемы и вызовы реализации. Несмотря на заметные шаги, мировая система управления искусственным интеллектом только формируется и сталкивается с серьёзными препятствиями. Первое – глубокий цифровой разрыв. Пока одни государства создают суперкомпьютеры и внедряют «зелёные» алгоритмы, другие не имеют базового доступа к сети. Без целенаправленной поддержки со стороны международных институтов новые инициативы рискуют закрепить неравенство. Второе – противоречие между суверенитетом и многосторонностью: страны по-разному понимают прозрачность, открытый код и потоки данных. Третье – отсутствие обязательности. И научная панель ООН, и рабочие группы БРИКС пока лишь дают рекомендации, не подкреплённые юридическими санкциями. Наконец, инициативы страдают от дефицита ресурсов: фонд доверия AIM представляет собой только первый шаг, а дальнейшая поддержка зависит от политической воли и экономической ситуации.

Заключение. Переход от принципов к реальным инструментам в международном управлении искусственным интеллектом показывает, что глобальное сообщество готово искать компромисс между развитием технологий и этическими ограничениями. ООН запускает независимые экспертные структуры и открытые платформы для диалога, не претендуя на роль наднационального регулятора. БРИКС, подчеркивая равенство и суверенитет, уже создаёт исследовательские центры, платформы и фонды для поддержки ИИ в странах Глобального Юга.

ШОС предлагает региональный контур сотрудничества, что важно для стран Центральной Азии. Для успеха всех этих начинаний нужны прозрачные правила, финансовая устойчивость и готовность государств делиться опытом без навязывания стандарта. Только так новые институты смогут превратить искусственный интеллект из источника конфликта в драйвер устойчивого развития.

Список источников и литературы:

1. Генеральная Ассамблея Организации Объединенных Наций. Резолюция 79/325 «Круг ведения и условия создания и функционирования Независимой международной научной группы по искусственному интеллекту и Глобального диалога по вопросам управления искусственным интеллектом» от 26 августа 2025 года. [Электронный ресурс] // Сайт «Организация Объединенных Наций». URL: https://docs.un.org/ru/A/RES/79/325 (дата обращения: 07.12.2025).
2. Мартиросян А. Ж. Глобальное управление искусственным интеллектом: рождение новой архитектуры или фрагментация «цифровой повестки»? 25.09.2025 [Электронный ресурс] // Сайт «РСМД» URL: https://russiancouncil.ru/analytics-and-comments/analytics/globalnoe-upravlenie-iskusstvennym-intellektom-rozhdenie-novoy-arkhitektury-ili-fragmentatsiya-tsif/ (дата обращения: 07.12.2025).
3. BRICS Leaders Call for Global AI Governance Rooted in Sovereignty, Equity, and South-South Cooperation [Электронный ресурс] // BABL AI. URL: https://babl.ai/brics-leaders-call-for-global-ai-governance-rooted-in-sovereignty-equity-and-south-south-cooperation (дата обращения: 19.10.2025).
4. From Alliance to Solutions: AIM Global 2025 Advances Inclusive and Sustainable Global Development [Электронный ресурс] // United Nations Industrial Development Organization (UNIDO). URL: https://www.unido.org/news/alliance-solutions-aim-global-2025-advances-inclusive-and-sustainable-ai-industry (дата обращения: 19.10.2025).
5. Independent International Scientific Panel on AI – Open Call for Candidates [Электронный ресурс] // United Nations. URL: https://www.un.org/independent-international-scientific-panel-ai/en/open-call (дата обращения: 19.10.2025).
6. Tianjin Declaration of the Council of Heads of State of the Shanghai Cooperation Organisation [Электронный ресурс] // Сайт «President of Russia» URL: http://en.kremlin.ru/supplement/6376 (дата обращения: 19.10.2025).
7. UN Advisory Body on Artificial Intelligence: Final Report – Governing AI for Humanity [Электронный ресурс] // Сайт «United Nations». URL: https://www.un.org/en/ai-advisory-body (дата обращения: 19.10.2025).

Ольга Олеговна Царькова,
студент 4 курса бакалавриата Института Международных Отношений,
Национальный Исследовательский Ядерный Университет «МИФИ»,
E-mail: carkovao43@gmail.com

Научный руководитель: Алексей Анатольевич Артамонов,
к.т.н., доцент кафедры анализа конкурентных систем,
Институт Международных Отношений,
Национальный Исследовательский Ядерный Университет «МИФИ»
E-mail: aaartamonov@mephi.ru

Olga O. Tsarkova,
fourth-year undergraduate student at the Institute of International Relations,
National Research Nuclear University MEPhI,
E-mail: carkovao43@gmail.com

Scientific supervisor: Alexey A. Artamonov,
Ph.D. in Technology, Associate Professor, Department of Competitive Systems Analysis,
Institute of International Relations,
National Research Nuclear University MEPhI
E-mail: aaartamonov@mephi.ru

ПОЗИЦИЯ КИТАЯ В МЕЖДУНАРОДНОМ РЕГУЛИРОВАНИИ И СОТРУДНИЧЕСТВЕ В СФЕРЕ ИИ: ВЛИЯНИЕ НА МИРОВОЙ ПОЛИТИЧЕСКИЙ ЛАНДШАФТ

CHINA'S APPROACH TO INTERNATIONAL AI GOVERNANCE AND COOPERATION: IMPACT ON THE GLOBAL POLITICAL LANDSCAPE

Аннотация. Автор рассматривает подход китайской политики в области ИИ на международной арене через анализ программы «Искусственный Интеллект +» (ИИ+), а также выдвинутых Китаем инициатив по глобальному регулированию на международных площадках. Китай выстраивает стратегию ИИ как основу экономического роста и как механизм усиления позиции в мире. Нормативный каркас сочетает внутреннюю индустриализацию ИИ с курсом на многосторонние стандарты под эгидой ООН, поддержку доступа стран Глобального Юга и развитие моделей ИИ с открытым исходным кодом. На фоне американского "AI Action Plan" китайский подход предлагает многостороннее сотрудничество вместо гонки, стремясь сократить технологический разрыв и укрепить международную легитимность собственных решений.

Ключевые слова: искусственный интеллект, Китай (КНР), ИИ+, сотрудничество, международное регулирование ИИ, управление ИИ, США, ШОС

Abstract. The author examines China's approach to AI policy on the international stage by analyzing the "Artificial Intelligence+" (AI+) programme and China's proposals for global AI governance initiatives in multilateral fora. China frames its AI strategy as a foundation for economic growth and as a mechanism for strengthening its global standing. The regulatory framework combines domestic AI industrialization with a commitment to multilateral standards under UN auspices, expanded access for countries of the Global South, and the development of open-source AI models. Against the U.S. "AI Action Plan," the Chinese approach emphasizes multilateral cooperation over a zero-sum race, seeking to narrow the technological gap and bolster the international legitimacy of its own policy choices.

Key words: artificial intelligence, China (PRC), AI+, cooperation, international regulation of AI, AI governance, USA, SCO

Китайская стратегия: ИИ как двигатель национального развития и инструмент глобального сотрудничества. Сегодня можно с уверенностью сказать, что Китай – один из ключевых игроков в сфере искусственного интеллекта (ИИ). Развитая инфраструктура и энергетика обеспечивают необходимые вычислительные мощности для ИИ, а общая нацеленность правительства не только на поддержку инноваций в данной области, но и на внедрение технологий ИИ в экономику, управление и сферу обеспечения безопасности создают благоприятные условия для роста объема научных исследований и доли соответствующих предприятий на рынке. Согласно данным Китайской академии информационных и коммуникационных технологий, на сентябрь 2025 года в Китае действовало более 5 тысяч профильных компаний, что составляет 15% от общемирового объема [2].

Китайские разработки в области ИИ конкурируют с западными аналогами и способны развиваться даже в условиях ограничений с американской стороны на ввоз чипов. Китаю удалось создать вторую по мощности вычислительную инфраструктуру в мире, что служит прочной основой для его цифровой экономики, а также позволяет задавать ориентиры для укрепления международного сотрудничества в этой сфере.

Пекин придает огромное значение вопросам сотрудничества и глобального управления в области искусственного интеллекта. С точки зрения Китая единые международные стандарты необходимы как для обеспечения глобальной безопасности, так и для снижения барьеров торговли и экспорта китайских технологий ИИ.

В 2023 году председатель КНР Си Цзиньпин вынес на рассмотрение глобальную инициативу по управлению искусственным интеллектом [4]. В данной инициативе закреплены основные принципы, на которые Китай и сегодня предлагает ориентироваться всему

международному сообществу в вопросе создания глобальной системы управления ИИ. Документ выдвигает одиннадцать ключевых принципов, призывающих к построению инклюзивного и справедливого мирового порядка в сфере ИИ, основанного на многостороннем сотрудничестве и уважении государственного суверенитета.

Данная инициатива задала основу китайской дипломатии в сфере ИИ, а ее основные положения по международному сотрудничеству нашли развитие в том числе и в новом ключевом стратегическом документе Китая – «Искусственный Интеллект +» («ИИ+»). Опубликованная Госсоветом КНР в августе 2025 года программа «ИИ+» нацелена на создание условий, в которых ИИ – основной драйвер экономического роста, а полное внедрение искусственного интеллекта во все сферы общества и экономики будет осуществлено до 2035 года [7].

Особый интерес представляет шестое предложение, вынесенное во второй раздел «Ускоренное осуществление ключевых действий», а именно – «Искусственный интеллект +» и глобальное сотрудничество». В этом пункте Китай обозначает две ключевые установки: 1) расширение международного партнерства и обеспечение широкого доступа к технологиям искусственного интеллекта, особенно для стран Глобального Юга; 2) совместное создание глобальной системы управления ИИ при поддержки ведущей роли ООН.

Другими словами, Китай ставит перед собой амбициозные цели и стремится использовать потенциал искусственного интеллекта, чтобы стимулировать рост национальной экономики и углубить международное сотрудничество в данной области.

От «гонки за лидерство» к формированию альтернативной модели глобального управления ИИ. Стремительная динамика китайской индустрии ИИ, подкрепленная национальными стратегиями и планами по достижению глобального лидерства в сфере ИИ, вызывает опасения со стороны США, страны-пионера в данной отрасли. Согласно исследованию Bruegel и MERICS, в котором рассматривается новизна патентов компаний Китая и США, Китай опережает в таких областях как компьютерное зрение и робототехника, но США по-прежнему удерживают лидерство в создании генеративного ИИ, машинном обучении, обработке естественного языка (NLP), а также применения ИИ в сфере кибербезопасности [3].

Несмотря на это, китайские компании быстро переняли опыт генеративных систем. В отличие от американских корпораций, которые не раскрывают код своих моделей, Китай стратегически ориентирован на политику открытого кода (Open-source).

В ранее описанной программе «ИИ+» отдельно подчеркивается важность развития проектов и инструментов open-source, обладающих международным влиянием. Для Китая создание и продвижение конкурентоспособных моделей с открытым исходным кодом – это долгосрочный план, который может обеспечить глобальное проникновение китайских ИИ

моделей. Продвижение своего открытого кода соответствует ключевому принципу китайской стратегии в области ИИ, которая рассматривает эту технологию как общественное благо и сферу, требующую развития международного сотрудничества.

В июле 2025 практически сразу после публикации Соединенными Штатами собственной стратегии «Достижение победы в конкурентной гонке в сфере искусственного интеллекта: план действий Америки в области ИИ», ("Winning the race: America's AI Action Plan" (AI Action Plan)), Китай представил на Всемирной конференции по искусственному интеллекту в Шанхае (WAIC) свой план совместного глобального регулирования ИИ. Заявление во многом стало ответным шагом Пекина на объявление США «гонки за искусственный интеллект» [5].

В то время как Вашингтон сосредоточился на снятии внутренних барьеров и усилении своего лидерства, китайская инициатива акцентировала необходимость многосторонних правил, недопущение превращения ИИ в «игру для избранных» из-за экспортных ограничений и санкций, а также устранение технологического разрыва между странами.

Расширение влияния Китая через механизмы ШОС, БРИКС и АСЕАН. Китайский подход на глобальной арене отличается стремлением вовлечь как можно больше стран, особенно развивающихся, в сотрудничество в сфере ИИ и совместную выработку норм. Китай заверяет, что готов делиться своим опытом и технологиями с другими государствами, особенно с Глобальным Югом, помогая им нарастить потенциал в сфере ИИ. Это логическое продолжение идеи ИИ как глобального общественного блага. Более того, Пекин предложил учредить Глобальную организацию по сотрудничеству в сфере ИИ – данная инициатива впоследствии была реализована в создании новой структуры под рабочим названием «Всемирная организация сотрудничества в области искусственного интеллекта» (World Artificial Intelligence Cooperation Organization (WAICO)), учреждение которой Китай инициировал также в июле 2025 года [6].

Особенно заметно усиление позиций Китая по вопросам ИИ в рамках Шанхайской организации сотрудничества (ШОС). В принятой на саммите в Тяньцзине (август 2025 года) декларации отмечается поддержка инициатив по созданию механизмов сотрудничества в области искусственного интеллекта и передовых технологий. Подразумевается, что одной из таких инициатив станет предложенный Си Цзиньпином Центр сотрудничества по внедрению ИИ для стран ШОС. Кроме этого, страны-участницы поддержали выполнение Дорожной карты по реализации Программы сотрудничества государств-членов ШОС по развитию искусственного интеллекта, принятую в июне 2025 в Чэнду; отметили предложение по использованию потенциала Международного центра искусственного интеллекта Alem.AI (инициатива Казахстана) по внедрению инноваций, а также согласились в необходимости укрепления научно-технического и инновационного сотрудничеств [1]. Вскоре после завершения саммита, в

Тяньцзине были открыты центры для практического сотрудничества с ШОС, а в Циндао – Центр научно-технического и инновационного сотрудничества Китай-ШОС, который будет заниматься в том числе совместными исследованиями искусственного интеллекта.

Схожая динамика прослеживается на площадках БРИКС и АСЕАН. Китай способствовал принятию совместной позиции БРИКС по ИИ, направленной на укрепление сотрудничества, а также создал Китайско-БРИКС центр развития и сотрудничества в области искусственного интеллекта. В рамках АСЕАН Китай продвигает Цифровой план действий «АСЕАН – Китай 2025», направленный на формирование устойчивого и справедливого партнерства в области ИИ.

Заключение. Подводя итог, можно отметить, что Китай не ограничился общими призывами, а начал формировать институциональные основы глобального управления ИИ. Он предлагает площадки и механизмы для международных консультаций, обмена опытом и выработки единых стандартов, при этом все еще поддерживая и акцентируя в своих предложениях ключевую роль ООН в данной области. Такой подход контрастирует с односторонними стратегиями, направленными на закрепление лидерства в сфере, апеллирует к идеалам равноправия и резонирует с запросом многих стран на коллективное решение вызовов ИИ. В результате Китай не только укрепляет свои позиции на международной арене, но и постепенно превращает собственное видение ИИ в неотъемлемую часть глобального политико-технологического дискурса XXI века.

Список источников и литературы:

1. Тяньцзиньская декларация Совета глав государств-членов Шанхайской организации сотрудничества [Электронный ресурс]. URL: https://rus.sectsco.org/images/07e9/09/01/1958599.pdf (дата обращения: 27.10.2025).

2. China's AI industry thrives with over 5,300 enterprises [Электронный ресурс] // The State Council of the People's Republic of China. URL: https://english.www.gov.cn/news/202510/01/content_WS68dce9d9c6d00ca5f9a06925.html (дата обращения: 27.10.2025).

3. García-Herrero A., Krystyanczuk M., Schindowski R. Which companies are ahead in frontier innovation on critical technologies? Comparing China, the European Union and the United States [Электронный ресурс]. // Bruegel Working Paper 08/2025. URL: https://www.bruegel.org/sites/default/files/2025-05/WP%2008.pdf (дата обращения: 27.10.2025).

4. Global AI Governance Initiative [Электронный ресурс] // Ministry of Foreign Affairs of the People's Republic of China. URL: https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367503.html (дата обращения: 27.10.2025).

5. Winning the Race: America's AI Action Plan [Электронный ресурс] // Washington, DC: The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (дата обращения: 27.10.2025).

6. Xu Ying. China's WAICO proposal and the reordering of global AI governance [Электронный ресурс] // China's Diplomacy in the New Era. URL: https://en.chinadiplomacy.org.cn/2025-07/30/content_118003645.shtml (дата обращения: 27.10.2025).

7. 国务院关于深入实施"人工智能+"行动的意见 [Электронный ресурс] // 中国政府网 URL: https://www.gov.cn/zhengce/content/202508/content_7037861.htm (дата обращения: 27.10.2025).

Алина Николаевна Щегрова,
студент 4 курса обучения,
Институт финансовых технологий и экономической безопасности,
Национальный исследовательский ядерный университет «МИФИ»,
E-mail: ashchegrova@bk.ru

Alina N. Shchegrova,
4th year student,
Institute for Financial Technologies and Economic Security,
National Research Nuclear University «MEPhI»,
E-mail: ashchegrova@bk.ru

ИНСТИТУЦИОНАЛИЗАЦИЯ ЭТИКИ: КАК КОРПОРАТИВНОЕ УПРАВЛЕНИЕ ДЕЛАЕТ ИСПОЛЬЗОВАНИЕ ИИ ОТВЕТСТВЕННЫМ

INSTITUTIONALIZATION OF ETHICS: HOW CORPORATE GOVERNANCE MAKES THE USE OF AI RESPONSIBLE

Аннотация. В статье исследуется роль корпоративного управления при минимизации этических и правовых рисков, связанных с внедрением искусственного интеллекта (ИИ) в бизнес-процессы. Автор доказывает, что эффективное корпоративное управление, в частности деятельность совета директоров, является ключевым механизмом институционализации этических принципов, трансформируя абстрактные нормы в обязательные элементы стратегии компании. Также подчеркивает необходимость развития цифровых компетенций в органах управления для обеспечения ответственного использования ИИ.

Ключевые слова: искусственный интеллект, этика ИИ, корпоративное управление, ответственный ИИ, цифровая трансформация.

Abstract. This article examines the role of corporate governance in minimizing the ethical and legal risks associated with the implementation of artificial intelligence (AI) in business processes. The author demonstrates that effective corporate governance, particularly the work of the board of directors, is a key mechanism for institutionalizing ethical principles, transforming abstract norms into mandatory elements of a company's strategy. The author also highlights the need to develop digital competencies in government bodies to ensure responsible use of AI.

Key words: artificial intelligence, AI ethics, corporate governance, responsible AI, digital transformation.

Основные риски, возникающие при использовании искусственного интеллекта в бизнесе. При изучении недавних конфликтных ситуаций, связанных с искусственным интеллектом,

например, использования ИИ при составлении аудиторского заключения компанией «Большой четверки» Deloitte для правительства Австралии и формировании отчета с фактическими и типографическими ошибками [1], можно определить ряд проблем, с которым может столкнуться бизнес. Так, согласно Абсалямовой Г.Ф. и Рафикову Р.И. [2], выделяются следующие виды риска:

– этико-алгоритмический: риски предвзятости, недостаточной прозрачности при формировании выводов и неподотчетности моделей ИИ, результатом которых могут стать несправедливые и дискриминационные решения;

– правовой и регуляторный: опасность утечек данных, нарушения законодательства о конфиденциальности и интеллектуальной собственности, а также растущее вмешательство государства, формирующего новое правовое поле для ИИ.

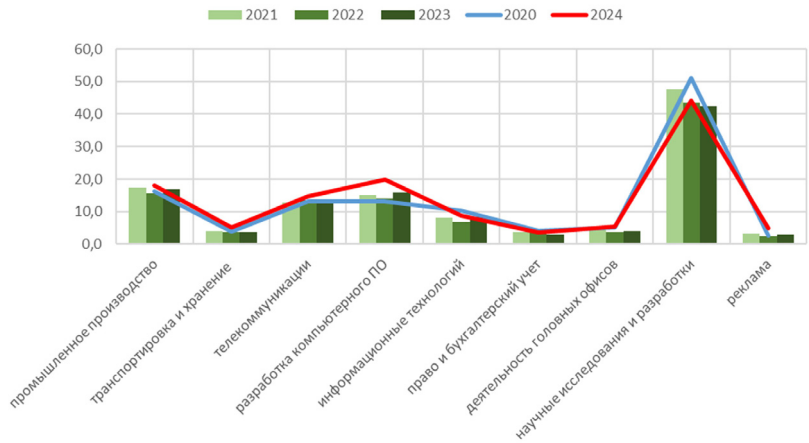
Горбачев Т.А. также выделяет среди многообразия угроз, возникающих на разных этапах использования Интеллекта, необходимость начальной обработки данных во избежание «…системных недочетов из-за низкого качества информации» [5, С. 99]. При этом даже качественные данные могут дать неправдоподобный результат из-за риска искажения в течение работы Модели или же ее необъяснимой концентрации на отдельных факторах.

Реализация некорректных алгоритмов искусственного интеллекта не только создаёт прямую угрозу информационной безопасности организации, но и подрывает фундамент клиентского доверия, что влечёт за собой существенные репутационные издержки, а также повышает вероятность судебных разбирательств и вмешательства регуляторных органов.

Таким образом, интеграция искусственного интеллекта в бизнес-процессы требует системного и всестороннего руководства – что находит отражение в разработанной ЮНЕСКО «Рекомендации об этических аспектах искусственного интеллекта». Согласно которой, «…государствам-членам и всем заинтересованным сторонам, включая частные предприятия [рекомендуется] обеспечить выполнение ими своих соответствующих обязательств…» [9] с целью работы систем ИИ на благо человека и общества.

Влияние корпоративного управления на процесс использования ИИ. В современной российской бизнес-среде, характеризующейся повышенным вниманием инвесторов и волатильностью доли цифровизации некоторых сфер экономической деятельности (рис. 1), а также отсутствием нормативного закрепления ответственного ведения бизнеса, абстрактные моральные принципы должны воплощаться в повседневной деятельности компании через систему корпоративного управления. Именно этот механизм способен трансформировать этику из рекомендации в обязательный элемент стратегического развития, обеспечивая не только экономическую эффективность, но и этическую целостность организации [8, 10, 6, 4].

Рисунок 1 – Доля инновационной активности некоторых видов экономической деятельности, %



Так, главный орган управления хозяйственных обществ – Совет директоров – определяет не только вектор развития компании, но и утверждает основополагающие документы: как отмечают исследователи «Сбер ПРО», именно технологические корпорации с 2016 года начали первыми разрабатывать и применять принципы использования ИИ, а к 2025г. более 1000 компаний (при этом в РФ зарегистрировано свыше 3,2 млн юридических лиц) подписали «Кодекс этики в сфере AI» – базу ответственного внедрения искусственного интеллекта в хозяйственную деятельность, основанную на принципах человекоцентричности, прозрачности и объяснимости алгоритмов, справедливости, безопасности и ответственности [3, 7].

В то же время, согласно исследованию [4], внедрение новых технологий в операционные процессы требует от компаний дополнительных ресурсов:

– постоянного контроля и совершенствования со стороны человека (например, в обязанности комитета по технологиям и инновационному развитию входит развитие направлений цифровой трансформации и проверка соответствия стандартам, стратегическим целям);

– повышения квалификации в области цифровизации и высоких технологий для членов Совета директоров (подавляющее большинство компаний-респондентов соответствующие программы не предусматривает);

– анализа результата использования ИИ: превалирующее число организаций не может предположить целесообразность внедрения технологии в текущие процессы.

Таким образом, современное корпоративное управление обеспечивает внутреннюю устойчивость при внедрении ИИ в бизнес-процессы, но требует совершенствования существующих подходов и большей мобильности.

Заключение. Проведенный анализ позволяет сделать вывод о том, что этические проблемы, связанные с использованием ИИ в бизнесе, носят системный характер, поэтому противодействие рискам сопровождаться не только провозглашением моральных принципов, но и конкретными мерами внутри корпораций, превалирующее число которых, как показывает практика, еще не готово к изменениям.

Список источников и литературы:

1. Deloitte заплатит Австралии из-за сделанного с ИИ отчета с ошибками. [Электронный ресурс]. Режим доступа: https://www.rbc.ru/technology_and_media/07/10/2025/68e4c63c9a79476d758073d8 (дата обращения: 01.11.2024).

2. Абсалямова Г.Ф., Рафиков Р.И. Преимущества и риски ИИ в бизнесе и рынке труда // Вопросы студенческой науки. – №05 (81). – май 2023. – С. 434–438.

3. Белая книга AI. Что нужно знать бизнесу об этике искусственного интеллекта. [Электронный ресурс]. Режим доступа: https://sber.pro/publication/belaya-kniga-ai-chto-nuzhno-znat-biznesu-ob-etike-iskusstvennogo-intellekta/ (дата обращения: 09.11.2025).

4. Внедрение информационных технологий и искусственного интеллекта в практику корпоративного управления: количественное исследование / М.Р Янковский; под ред. А.Я. Граница, В.А. Лоскутов, С.А. Поршаков, А.А. Тимошенко, Е.В. Чумакова; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2023. – 66 с.

5. Горбачев Т.А. Искусственный интеллект: риски и проблемы внедрения в Российской Федерации // Инновационная экономика: информация, аналитика, прогнозы. – 2025. – №1. – С. 96–105.

6. Зуб А.Т., Петрова К.С. Искусственный интеллект в корпоративном управлении: возможности и границы применения // Государственное управление. Электронный вестник. – 2022. – №94. – С. 173–187.

7. Количество зарегистрированных юридических лиц и индивидуальных предпринимателей. [Электронный ресурс]. Режим доступа: https://service.nalog.ru/gosreg/statistics.html (дата обращения: 09.11.2025).

8. Ответственное ведение бизнеса. [Электронный ресурс]. Режим доступа:https://economy.gov.ru/material/directions/vneshneekonomicheskaya_deyatelnost/mnogostoronnee_ekonomicheskoe_sotrudnichestvo/oesr/otvetstvennoe_vedenie_biznesa/ (дата обращения: 05.11.2025).

9. Рекомендация об этике искусственного интеллекта, принята 23.11.2021 на 41-й сессии Генеральной конференции ЮНЕСКО. - Париж: ЮНЕСКО, 2021. - [Электронный ресурс]. Режим доступа: https://unesdoc.unesco.org/ark:/48223/pf0000380455_rus (дата обращения: 01.11.2024).

10. Щербаченко П.С. Роль совета директоров в реализации концепции корпоративной социальной ответственности // Вестник университета. – 2013. – № 8. – С. 179–186.

Секция А2

«Цифровая дипломатия, медиа и трансформация международных отношений»

Ангелина Владимировна Тарасенко,
студент 1 курса магистратуры факультета международных отношений по направлению Дипломатия Российской Федерации и зарубежных государств,
Санкт-Петербургский государственный Университет,
E-mail: angelinatarasenko018@gmail.com

Angelina V. Tarasenko,
1st year master's student of the Faculty of International Relations in the field of Diplomacy of the Russian Federation and Foreign States,
Saint Petersburg State University,
E-mail: angelinatarasenko018@gmail.com

РОЛЬ ЦИФРОВОЙ ДИПЛОМАТИИ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ В XXI ВЕКЕ

THE ROLE OF DIGITAL DIPLOMACY IN ENSURING CYBERSECURITY IN THE XXI CENTURY

Аннотация. Цифровая дипломатия развивается как ответ на новые вызовы и возможности, порожденные быстрым развитием информационных технологий. Она предполагает не только использование цифровых платформ для коммуникаций, но и привлечение технических экспертов, аналитиков данных и специалистов по безопасности для выработки совместных мер. Кибердипломатия как специализированное направление направлена на предотвращение киберинцидентов путем формирования доверия между государствами и контролируемого обмена информацией о возникших угрозах.

В рамках исследования будут рассмотрены основные характеристики и этапы развития цифровой дипломатии, её роль в обеспечении безопасности на государственном и международном уровнях. Вызовы, связанные с историей и актуальными вызовами касательно цифровой дипломатии, будут представлены практические примеры стран-лидеров в области кибердипломатии. Анализ деятельности ведущих держав в области цифровой дипломатии, позволит выявить направления дальнейшего совершенствования дипломатических методов для адаптации к быстро меняющемуся цифровому ландшафту. Особое внимание уделено влиянию этих процессов на формирование международной безопасности и стабильности информационного пространства.

Ключевые слова: Цифровая дипломатия, социальные сети, информационное пространство, Россия, кибердипломатия, международные отношения.

Abstract. Digital diplomacy is developing as a response to new challenges and opportunities generated by the rapid development of information technology. It involves not only the use of digital platforms for communication, but also the involvement of technical experts, data analysts and security specialists to develop joint measures. Cyber diplomacy as a specialized field is aimed at preventing cyber incidents by building trust between States and the controlled exchange of information about emerging threats.

The study will examine the main characteristics and stages of the development of digital diplomacy, its role in ensuring security at the national and international levels, as well as challenges related to the history and current challenges regarding digital diplomacy, practical examples of leading countries in the field of cyber diplomacy will be presented. An analysis of the activities of the leading powers in the field of digital diplomacy will identify areas for further improvement of diplomatic methods to adapt to the rapidly changing digital landscape. Special attention is paid to the impact of these processes on the formation of international security and the stability of the information space.

Key words: Digital diplomacy, social networks, information space, Russia, cyber diplomacy, international relations.

Понятие цифровой дипломатии и ее эволюция. В начале 2010-х годов появилось новое направление в области международных отношений, связанное с использованием цифровых технологий для обмена информацией, анализа данных и координации действий. Оно охватывает более широкий спектр процессов, чем традиционные практики, и включает управление потоками больших объемов информации с целью поддержки диалога между государствами и международными организациями. Важным элементом этой трансформации стало активное использование данных в дипломатической деятельности. Дипломаты стали не только передавать ноты, но и собирать, систематизировать и анализировать цифровые массивы, чтобы вырабатывать более точные и оперативные решения. Это направление получило отдельное название, подчеркивающее роль информации как ресурса и инструмента влияния в развитии международных отношений.

Термин *цифровая дипломатия,* распространенный наряду с понятиями интернет-дипломатия, дипломатия социальных сетей и Web 2.0 дипломатия, впервые начал использовать применительно к внешней политике США. В частности, под ним подразумевалось широкое использование информационно-коммуникационных технологий (ИКТ), в том числе новые медиа, социальных сетей, блогов и тому подобных медиаплощадок в глобальной сети для содействия государственным органам для осуществления функций и коммуникаций по вопросам, связанным с внешнеполитической повесткой дня [2].

Правительство США определяет цифровую дипломатию как применение социальных сетей в дипломатической практике правительства США для обеспечения взаимодействия американских дипломатов с зарубежными пользователями интернета [5].

В 2010-2011 гг. Белым домом были опубликованы несколько официальных документов, задающих направления цифровой дипломатии. В их числе был документ «Публичная дипломатия: укрепление взаимодействия Соединенных Штатов с миром» [7]. В данном документе обозначились задачи, определяемые руководством США для цифровой дипломатии. В частности, в список таких задач вошли:

1. Дискредитация идеологических противников Соединенных штатов;
2. Противодействие информационной деятельности Китая в интернете;
3. Ограничение медиа преступности России на пространстве бывшего Советского Союза;
4. Противодействие внешней культурной политике Ирана, осуществляемой через социальные сети [4].

В рамках социальных сетей и информационного пространства идея цифровой дипломатии разрослась за счет внедрения аналитики больших данных, кибербезопасности и инновационных методов ведения переговоров. Этот процесс сопровождался формированием новых стандартов и правил, регулирующих поведение в цифровом пространстве.

Реализация программ цифровой дипломатии предполагает следующие направления деятельности:

1. Финансирование проектов по созданию и распространению новых технологий, позволяющих обходить цензуру в сети;
2. Создание информационных сервисов, направленных на поддержку оппозиции в авторитарных странах;
3. Создание систем теневого интернета и независимых сетей мобильной связи, развертывание которых на территории третьих стран позволит борцам с авторитарными режимами обмениваться информацией в режиме онлайн, обходя запреты властей [1].

В результате цифровая дипломатия вышла за рамки простого технического инструмента и превратилась в комплексную область, объединяющую информационные технологии, международное право, политические интересы и стратегию безопасности. Современный уровень развития этой сферы демонстрирует, насколько изменились методы и механизмы взаимодействия, став адаптивными к вызовам цифрового века. Таким образом, цифровая дипломатия стала фундаментом для новых форм международного сотрудничества.

Кибердипломатия как инструмент обеспечения безопасности. Следующим шагом эволюции цифровых практик стала кибердипломатия- специализированная область дипломатии, направленная на управление киберрисками и предотвращение конфликтов в цифровом пространстве. В отличие от общего использования цифровых технологий в международных отношениях, кибердипломатия фокусируется на выработке правил поведения и согласованных действий, направленных на снижение угроз, связанных с вредоносными кибероперациями, шпионажем и дестабилизацией критически важных информационных систем. Дипломаты в области кибербезопасности участвуют в создании и поддержке международных стандартов безопасности, которые охватывают технические, юридические и этические аспекты использования киберпространства. Работа в рамках дипломатии в кибербезопасности включает не только реагирование на инциденты, но и превентивное планирование, основанное на анализе тенденций и прогнозировании развития угроз. Это позволяет формировать проактивные стратегии, направленные на укрепление устойчивости информационных систем и снижению уязвимостей. Обсуждение этих вопросов происходит в специализированных форматах, таких как международные конференции, рабочие группы и совместные тренировки, усиливающие сотрудничество и обмен опытом.

Если рассматривать потенциал цифровой дипломатии для России необходимо с учетом нынешней роли и потенциала дальнейшего развития информационного сектора для отечественной экономики, национальной безопасности, системы государственного управления. На сегодняшний день РФ является одним из наиболее динамичных и устойчиво растущих ИТ-рынков в мире [6].

В современное время и с нынешним положением на мировой арене цифровая дипломатия в РФ кардинально изменилась. Россия столкнулась с большим количеством интернет-кампаний с западного информационного пространства, направленных на дискредитацию имиджа лидеров России, гражданского населения и государственных институтов, что представляют значительный вызов для цифровой дипломатии не только для России, но и для мирового пространства.

Профили российских каналов международного вещания стали чрезвычайно активными в Twitter (признана экстремистской и запрещена на территории РФ) после начала СВО, даже по сравнению с их собственной активностью на российской платформе VK. Это указывает на подвижки в стратегии цифровой дипломатии России: больше внимания и усилий было приложено, чтобы эффективно осуществлять информационные кампании среди глобальной аудитории. Россия, несмотря на ограничение работы на зарубежных платформах, сумела увеличить распространение своих взглядов среди зарубежной аудитории. Если в период с 1 января 2021 г. По 24 февраля 2022 г. Каналы международного вещания России, отвечающие за

цифровой контент и распространение пророссийской позиции, опубликовали 22 тысячи постов, то только за период с 24 февраля 2022 г. По 15 мая 2022 г., то есть за три месяца, было опубликовано уже 36 тысяч постов на платформе Twitter (признана экстремистской и запрещена на территории РФ) [3].

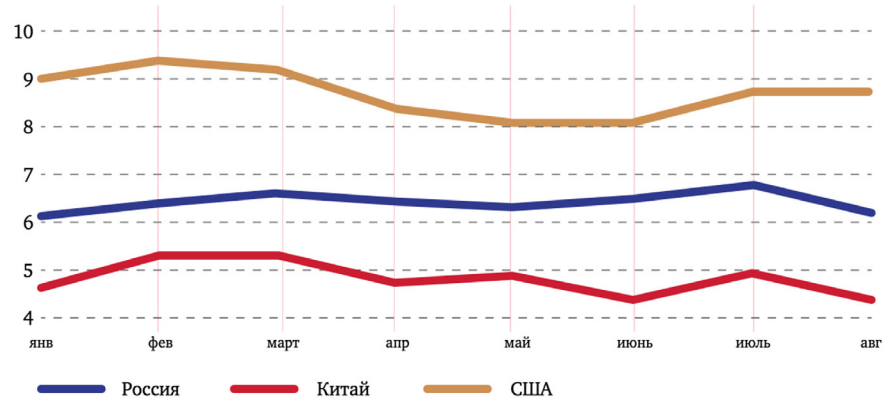


Диаграмма 1: Показатель эффективности охвата пользователей цифровой дипломатией России, Китая, США, январь-август 2023 г [3].

Проанализировав из этой диаграммы и тенденциями современных международных отношений:

Соединённые Штаты, например, активно используют платформы многостороннего обмена информацией о киберугрозах, таких как Forum of Incident Response and Security Teams (FIRST) и международные коалиции по кибербезопасности. Их стратегии включают адаптивное реагирование на инциденты и систематическое внедрение протоколов обмена разведданными, что позволяет оперативно выявлять и нейтрализовать угрозы на ранней стадии.

Китай продвигает концепцию «киберсуверенитета», акцентируя внимание на праве каждого государства контролировать и регулировать свои национальные цифровые ресурсы. В рамках этой политики страна развивает инфраструктуру, обеспечивающую мониторинг, фильтрацию и контроль интернет-трафика, а также активно участвует в формировании международных норм, отражающих эти принципы. При этом Пекин поддерживает двусторонние и многосторонние договоренности, направленные на совместное противодействие киберугрозам, уделяя внимание развитию технических стандартов и обмену информацией на государственном уровне.

Российская Федерация осуществляет комплексный подход, объединяя элементы национальной стратегии информационной безопасности с активным цифровым

представительством на международной арене. Важным инструментом становится сотрудничество в рамках Организации Договора о коллективной безопасности (ОДКБ), Шанхайской Организации Сотрудничества (ШОС), БРИКС, а также участие в группе правительственных экспертов (ГПЭ ООН) по вопросам информационной безопасности и группе высокого уровня по цифровому сотрудничеству ООН (ГВУЦ) под эгидой Генсекретаря для координации глобальной цифровой повестки. Москва придает большое значение развитию механизмов контроля над распространением вредоносного программного обеспечения и совершенствованию процедур расследования киберинцидентов через цифровую дипломатию.

Заключение. В работе поставлена задача выявить ключевые механизмы, обеспечивающие эффективное международное сотрудничество и формирование нормативных актов, способствующих снижению рисков конфликтов и укреплению глобальной стабильности.

Практика ведущих государств показала широкий спектр подходов и инструментов – от технических платформ обмена информацией до национальных политик, учитывающих особенности цифрового суверенитета и безопасности. Эти примеры продемонстрировали важность сбалансированного сочетания технологических возможностей и политических решений для эффективного управления киберрисками.

В результате исследования было выявлено, что дипломатия выступает не просто посредником, а активным участником формирования глобальной архитектуры кибербезопасности. Её способность объединять государства вокруг общих норм и ценностей, адаптироваться к быстроменяющимся условиям и предотвращать конфликты играет решающую роль в сохранении стабильности информационного пространства. Таким образом, дальнейшее развитие цифровой дипломатии (использование соцсетей, вебсайтов и блогов) и кибердипломатии (занимающиеся вопросами безопасности в информационном пространстве), а также совершенствование международного сотрудничества являются необходимыми условиями для успешного противодействия современным вызовам безопасности в цифровую эпоху.

Список источников и литературы:

1. Федеральная целевая программа «Электронная Россия (2002–2010 годы)». Юридическая компания «Интернет и право». 2010, 2 марта, http://www.internet-law.ru/intlaw/laws/e-rus.htm (Дата обращения: 11.12.2025).
2. Цветкова Н. Программы Web 2 в публичной дипломатии США. США и Канада: Экономика, политика, культура. 2011 № 3 С. 109-122.
3. «Цифра» и искусственный интеллект на службе дипломатии: аналитический доклад/ [Е.С. Зиновьева, Н.А. Цветкова, А.Н. Сытник и др.; под ред. Е.С. Зиновьевой] — М.: МГИМО, 2024. — 47 с.

4. Черненко Е. Интернет-протокольная служба Госдепа. Газета Коммерсантъ. 2011, 15 сентября, http://www.kommersant.ru/doc/1773567/print (Дата обращения: 11.12.2025).
5. IT Strategic Plan: Fiscal Years 2011–2013 Digital Diplomacy. US Department of State. 2010 September 1, http://www.state.gov/m/irm/rls/148572.htm (Дата обращения: 12.11.2025).
6. Public Diplomacy: Strengthening U. S. Engagement with the World. A Strategic Approach for the 21st Century, 2010 http://www.carlisle.army.mil/DIME/documents/Public%20%20Diplomacy%20%20%20US%20%20%20World%20%20Engagement.pdf (Дата обращения: 11.12.2025).
7. Park, C. Y., et al. (2022). VoynaSlov: A Data Set of Russian Social Media Activity during the 2022, https://www.researchgate.net/publication/360859819_VoynaSlov_A_Data_Set_of_Russian_Social_Media_Activity_during_the_2022_Ukraine-Russia_War (Дата обращения: 11.12.2025).

Арина Игоревна Горячева,
преподаватель кафедры мировой экономики,
международных отношений и права,
Новосибирский государственный университет
экономики и управления «НИНХ»
E-mail: a.i.goryacheva@nsuem.ru

Arina Igorevna Goryacheva,
Lecturer, Department of World Economy,
International Relations, and Law,
Novosibirsk State University of Economics and Management "NINH"
Email: a.i.goryacheva@nsuem.ru

НОВЫЕ МЕДИА И ЦИФРОВАЯ ДИПЛОМАТИЯ: ТРАНСФОРМАЦИЯ КОММУНИКАЦИОННЫХ СТРАТЕГИЙ В СОВРЕМЕННОМ МИРЕ

NEW MEDIA AND DIGITAL DIPLOMACY: TRANSFORMING COMMUNICATION STRATEGIES IN THE MODERN WORLD

Аннотация. Современный мир сложно представить без новых средств коммуникации. Развитие и внедрение ИКТ во все сферы жизни общества оказало значительное влияние на коммуникационные процессы. Благодаря Интернету появляется возможность сделать коммуникацию быстрой, глобальной и доступной. Цифровая революция трансформирует средства коммуникации в современном мире. В конце XX века появляется термин «новые медиа». С возрастанием популярности цифровых ресурсов, они внедряются во всех сферы жизни общества, включая политическую. Широкое использование новых медиа в политической коммуникации привело к появлению в XXI веке термина «цифровая дипломатия». В работе анализируется понятие «цифровая дипломатия», описаны возможности нового вида дипломатической деятельности. Также в работе исследована тесная связь между такой дипломатией и новыми медиа. Определено, что цифровая дипломатия реализуется с помощью новых медиа, что создает возможности для эффективного взаимодействия между государством и общественностью. В работе также анализируются ресурсы цифровой дипломатии Российской Федерации.

Ключевые слова: цифровая дипломатия, новые медиа, социальные сети, цифровизация, онлайн-СМИ, цифровые технологии, политическая коммуникация.

Abstract. It's hard to imagine the modern world without new means of communication. The development and implementation of ICT in all spheres of society has significantly impacted communication processes. The internet makes communication fast, global, and accessible. The digital revolution is transforming modern communication. The term "new media" emerged at the end of the 20th century. With the growing popularity of digital resources, they are being integrated into all spheres of society, including politics. The widespread use of new media in political communication led to the emergence of the term "digital diplomacy" in the 21st century. This paper analyzes the concept of "digital diplomacy" and describes the potential of this new type of diplomatic activity. The close connection between digital diplomacy and new media is also explored. It is determined that digital diplomacy is implemented through new media, creating opportunities for effective interaction between the state and the public. The paper also analyzes the digital diplomacy resources of the Russian Federation.

Key words: digital diplomacy, new media, social networks, digitalization, online media, digital technologies, political communication.

Средства массовой информации с самого своего появления всегда играли особую роль в жизни общества. СМИ не только информируют людей о происходящих событиях, но и формируют их ценности, взгляды, предпочтения и даже привычки. В XXI цифровизация активно внедряется во все сферы общества, не оставив без внимания и средства массовой информации. В новом тысячелетии интернет-технологии трансформируют традиционные СМИ. Благодаря развитию ИКТ появляются так называемые «новые медиа» (онлайн-медиа), включающие в себя сайты, социальные сети, блог-платформы, микроблоги и др. Все большее количество людей из разных уголков планеты отдают предпочтения именно им. Читатели выбирают онлайн-медиа по разным причинам, среди их основных достоинств можно отметить: оперативность; интерактивность; круглосуточный доступ к информации; наличие обратной связи; возможность выбрать интересующий контент; отсутствие географических границ и др. [5, с. 235].

Некоторые исследователи предполагают, что через некоторое время новые медиа полностью заменят собой традиционные СМИ. Согласно отчету «Global digital 2025» сегодня в мире насчитывается 5,56 миллиарда пользователей интернета [8]. Это означает, что 67,9% мирового населения имеют доступ к Интернету. За 2024 год количество интернет-пользователей увеличилось на 1.7% [7].

Роль новых медиа продолжает активно возрастать [6, с. 2]. Важное значение цифровые ресурсы приобретают и в политической коммуникации [1, с. 82]. Практика использования новых медиа в политической сфере привела к появлению нового феномена, именуемого «цифровой дипломатией» в отечественной литературе или «digital diplomacy» в работах зарубежных исследователей.

Впервые данный термин был определен в работе американского журналиста У.Дизарда «Цифровая дипломатия: американская внешняя политика в эпоху информации» в 2001 году [9]. Однако предпосылки внедрения цифровой дипломатии различными государствами можно увидеть раньше. Так, например, 20 октября 1994 года был создан официальный веб-сайт Белого дома, что стало отправной точкой для правительств в использовании Интернета. В настоящий момент термин получил широкое распространение, как в зарубежном, так и отечественном дискурсе. Рассмотрим несколько определений данного понятия.

Американский исследователь Ф.Хэнсон определяет новый вид дипломатической деятельности следующим образом: «цифровая дипломатия – реализация достижения дипломатических целей с помощью использования ИКТ и социальных сетей» [10].

Директор Департамента информации и печати, официальный представитель МИД России, член Коллегии МИД России М.В.Захарова характеризует термин следующим образом: «Цифровая дипломатия – внешнеполитическая деятельность, осуществляемая с помощью информационно-коммуникационных технологий и возможностей цифровых платформ, целью, которой является продвижение и защита национальных интересов Российской Федерации в мировом информационном пространстве» [3].

Исходя из описанных выше определений можно сделать вывод о том, что инструментами реализации цифровой дипломатии являются новые медиа, к ним относятся: сайты, блоги, социальные сети и другие онлайн-ресурсы в сети Интернет. Использование онлайн-медиа в дипломатической коммуникации предоставляет множество преимуществ, среди которых: возможность общаться с аудиторией без посредников; транслировать официальную государственную позицию, минуя искажение информации различными СМИ; позволяет публиковать и обновлять информацию за считанные секунды; создает возможность двусторонней коммуникации, что позволяет получать обратную связь от аудитории; гарантирует большую прозрачность, что способствует укреплению доверия общественности [2, с. 137].

В Российской Федерации цифровая дипломатия активно развивается примерно с 2010-х годов [3]. Министерство иностранных дел Российской Федерации активно развивает свой сайт, социальные сети и мессенджеры. Сайт Министерства иностранных дел Российской Федерации активно просматривают как граждане РФ, так и представители других стран. Например, в октябре 2025 года на сайт больше всего заходили посетители следующих стран: Россия (327 186 ч.), Беларусь (244 898 ч.), Казахстан (11 293 ч.), Узбекистан (4 433 ч.), Молдова (3 599 ч.), Израиль (3099 ч.), Кыргызстан (2698 ч.), Латвия (2597 ч.), Иран (2217 ч.), Эстония (2033 ч.) (Рис. 1). В настоящее время МИД РФ официально представлен на 12 цифровых платформах на четырех языках [3].

Название	Просмотры	Посетители	Визиты	Отказы
Всего	1 027 759	327 186	393 114	81 164
Россия	834 246	244 898	289 701	55 990
Беларусь	17 137	11 293	12 075	2 552
Казахстан	12 225	8 125	8 617	1 731
Узбекистан	5 727	4 433	4 625	891
Молдова	4 789	3 599	3 789	794
Израиль	4 786	3 099	3 354	706
Кыргызстан	4 003	2 698	2 885	658
Латвия	5 680	2 597	3 512	1 004
Иран	11 891	2 217	7 229	2 906
Эстония	3 282	2 033	2 179	532

Рис. 1 Посещаемость сайта Министерства иностранных дел Российской Федерации по географическому критерию (октябрь 2025 года)

На сайте предоставлена информация о деятельности МИД, размещены официальные документы, новости, официальные заявления, полезная информация и многое другое. А также в разделе «пресс-служба» представлены другие ресурсы цифровой дипломатии России: социальные сети посольств и консульств, постоянные представительства, территориальные представительства, персональные аккаунты российских дипломатов [4].

Еще одним элементом цифровой дипломатии Российской Федерации являются личные аккаунты и блоги политических деятелей. В современных реалиях политические деятели РФ, как правило, отдают предпочтения телеграм-каналам. Согласно данным TGStat, наибольшее количество подписчиков в «Телеграм» имеет глава Чечни Р.А.Кадыров, количество подписчиков его канала составляет 2 млн. 43 тыс. человек [11]. Второе место в рейтинге занимает еще один популярный российский политический деятель РФ – Д.А.Медведев, количество подписчиков на его канале достигло отметки 1 млн. 817 тыс. Однако по охвату и цитируемости публикаций Дмитрий Анатольевич является лидером (Рис. 2). Тройку лидеров по количеству подписчиков замыкает российский государственный деятель А.С.Делихманов, в настоящий момент канал имеет 1 млн. 675 тыс. подписчиков (Рис. 2). Активно ведет свой канал и председатель государственной думы Российской Федерации В.В.Володин, количество его подписчиков составляет 1 млн. 371 тыс. А также директор департамента информации и печати Министерства иностранных дел Российской Федерации М.В.Захарова, количества подписчиков ее авторского канала более 521 тыс. человек [11].

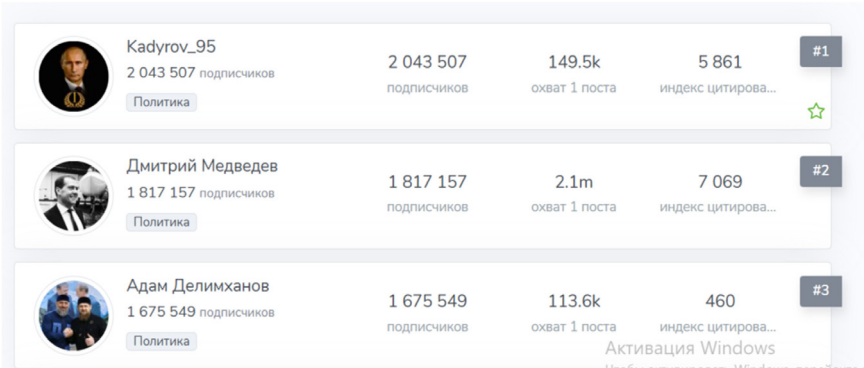


Рис. 2. Телеграм-каналы российских государственных и политических деятелей (октябрь 2025 года)

Заключение. Таким образом, в современных условиях роль новых медиа продолжает расти и завоевывать внимание общественности. В XXI веке новые медиа активно внедрялись и в политическую коммуникацию, что способствовало появлению нового феномена, именуемого цифровой дипломатией. Новые медиа неотделимы от цифровой дипломатии, так как именно через них реализуются главные задачи современной дипломатии в цифровую эпоху. В текущих условиях государствам важно уделять достаточно внимание внедрению и развитию цифровой дипломатии. Однако важно не только вести сайты и социальные сети, но и учитывать обратную связь и эффективность этих ресурсов.

Список источников и литературы:

1. Балчугов А. В. «Новые медиа» в современной российской политике: преимущества и потенциал / А. В. Балчугов, А. Е. Белянцев, Р. В. Бугров, О. А. Немцова // Власть. 2019. Т. 27, № 3. С. 82-85.

2. Борисов, Д. А. Значение цифровой дипломатии в эпоху многополярности / Д. А. Борисов, А. И. Горячева // Ученые записки Крымского федерального университета имени В.И. Вернадского. Философия. Политология. Культурология. 2025. Т. 11, № 2. С. 134-150.

3. Лекция Марии Захаровой «Цифровая дипломатия МИД России» [электронный ресурс] // МГИМО. 2024. 28 мая. URL: https://mgimo.ru/about/news/departments/zakharova-mfa-digital-diplomacy/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 27.20.2025).

4. Министерство иностранных дел Российской Федерации [Электронный ресурс]. URL: https://mid.ru/ru/ (дата обращения 06.11.2025).

5. Тулисова В. А. Трансформация средств массовой коммуникации: от традиционных средств массовой информации к New Media // Вопросы теории и практики журналистики. 2017. №2. С. 228-244. URL: https://cyberleninka.ru/article/n/transformatsiya-sredstv-massovoy-kommunikatsii-ot-traditsionnyh-sredstv-massovoy-informatsii-k-new-media (дата обращения: 21.10.2025).

6. Шестова, Т. Л. Новые медиа в современном политическом процессе / Т. Л. Шестова, В. А. Кузьмин // Социально-гуманитарные знания. 2019. № 4. С. 1-4. URL: https://elibrary.ru/download/elibrary_39554235_10340249.pdf (дата обращения: 21.10.2025).

7. Digital 2024: global overview report [Electronic resource]. URL: https://datareportal.com/reports/digital-2024-global-overview-report (acsessed 16.10.2025).

8. Digital 2025: global overview report [Electronic resource]. URL: https://datareportal.com/reports/digital-2025-global-overview-report (acsessed 16.10.2025).

9. Dizard W.P. Digital diplomacy: U.S. foreign policy in the information age. Westport, Praeger, 2001, 356 p.

10. Hanson, F. Revolution @State: The Spread of Ediplomacy (2012) [Electronic resource]. URL: https://www.brookings.edu/wp-content/uploads/2016/06/03_ediplomacy_hanson.pdf (accessed 01.11.2025).

11. TGSTAT.RU [Electronic resource]. URL: https://tgstat.ru/ (accessed 07.11.2025).

Дарья Анатольевна Сальникова,
магистрант 2 курса факультета управления и политики,
МГИМО МИД России,
E-mail: da.a.salnikova@my.mgimo.ru

Daria An. Salnikova,
2nd year Master's student at the School of Governance and Politics,
MGIMO University,
E-mail: da.a.salnikova@my.mgimo.ru

НА ПУТИ К ЦИФРОВОЙ ДИСЦИПЛИНЕ

TOWARDS DIGITAL DISCIPLINE

Аннотация. Статья посвящена политическому и правовому регулированию внедрения технологий искусственного интеллекта (ИИ) в России. Автор рассматривает позиции ведущих парламентских партий по вопросам использования и регулирования ИИ, а также проводит анализ инициатив в области цифровизации. Особое внимание уделяется политическим рискам и этическим вопросам, связанным с расширением применения «цифрового разума». Автор отмечает, что, несмотря на активность партий в продвижении цифровых проектов, законодательная база не поспевает за технологическим развитием. Автор приходит к выводу о необходимости межфракционного взаимодействия и системного подхода к регулированию ИИ для сохранения технологического лидерства России и обеспечения безопасности граждан.

Ключевые слова: искусственный интеллект, политические партии, «Единая Россия», ЛДПР, КПРФ, «Новые люди», Государственная Дума, регулирование ИИ, технологическое лидерство, цифровой суверенитет

Abstract. The article is devoted to the political and legal regulation of the implementation of artificial intelligence (AI) in Russia. The author examines the positions of Russian parliamentary parties on the use and regulation of AI, as well as analyzes initiatives in the field of digitalization. Special attention is paid to the political risks and ethical issues associated with the expansion of the use of digital intelligence. The author notes that despite the parties' activity in promoting digital projects, the legislative framework has not kept in step with technological development. The author concludes that there is a need for inter-factional interaction and a systematic approach to AI regulation in order to preserve Russia's technological leadership and ensure the safety of citizens.

Keywords: artificial intelligence, political parties, “United Russia”, LDPR, CPRF, “New People”, State Duma, AI regulation, technological leadership, digital sovereignty

Развитие технологий искусственного интеллекта (ИИ) – предмет политических, правовых и этических споров. Технология стала неотъемлемой частью промышленности, строительства, медицины, образования, госуправления и военной сферы. Современные информационные и когнитивные войны нельзя представить без ИИ. Кроме того, нейросети добрались и до творческих профессий: с актрисой Тилли Норвуд хотят сотрудничать сразу несколько голливудских агентств. Правда, есть нюанс: Норвуд не существует в реальности, ведь она – сгенерированная ИИ модель студии Xicoia [5]. В современных условиях перед государством стоит вопрос: какие сферы можно безопасно делегировать «цифровому разуму», а где чрезмерное использование технологии может навредить.

Известно, что Россия является одним из мировых лидеров по внедрению ИИ, а отечественные достижения в области высоко оцениваются за рубежом. В стране активно развиваются платформенная экономика и цифровой рубль, а российский финтех бьет все рекорды: например, Сбер стал лидером рейтинга крупнейших мировых эквайеров, обогнав JPMorgan Chase и Worldpay [6].

Политические партии ожидаемо не остаются в стороне при обсуждении трендов внедрения ИИ: внимание уделяется регулированию применения технологии и ее последствий. Среди главных рисков, с которыми парламентарии стремятся бороться, – утечка информации и корпоративных переписок, доминирование западной повестки в зарубежных генеративных моделях, а также «когнитивные травмы», при которых человек, выполняющий всю работу с помощью ИИ, становится зависимым и теряет способность работать и даже думать самостоятельно.

Наиболее активный (по числу внесенных инициатив) «игрок» в этой сфере – партия «Новые люди», которая выдвигает весьма много инициатив, связанных с цифровизацией в целом, и рассматривает передовые технологии как один из столпов своей программы. Наиболее успешный проект партии – введение цифрового контроля «Мигрант ID». Инициатива нашла поддержку среди граждан и стала основным инструментом контроля за мигрантами в новой Концепции государственной миграционной политики до 2030 года. Вместе с тем другие предложения партии «технократов» в сфере внедрения ИИ менее глобальны и не получают столь масштабной поддержки [4].

Второе место по активности на ИИ-треке занимает «Единая Россия». К темам, которые проходят красной нитью в инициативах партии, относятся защита россиян от кибермошенников, противодействие использованию технологии в искажении информации (например, дипфейки) и эффективное отраслевое применение ИИ. «Хордовой идеей» данной партии является выстраивание цифрового суверенитета России [7].

Другая важная тема, на которую делает акцент партия «Единая Россия» – ограничение использования ИИ в «чувствительных сферах» [2]. Несколько лет назад партия представила «Цифровой манифест» – документ, запрещающий государству передавать ключевые функции и право принятия решения «цифровому разуму» в областях, затрагивающих конституционные права граждан – медицине, юриспруденции, образовании [3]. Несмотря на то, что дальнейшего развития «манифест» не получил, «Единая Россия» решила включить тематику ИИ и его внедрение в некоторые социальные сферы «Народной программы», а платформой для «цифрового ликбеза» граждан выступает партпроект «Цифровая Россия». При этом попытки «ЕР» разработать законопроект по регулированию ИИ, пока не увенчались успехом.

«Справедливая Россия» замыкает тройку лидеров по числу внесенных инициатив. Выступает за выработку четких нормативно-правовых рамок применения ИИ-технологий. Партия, среди прочего, вносила в Госдуму законопроект с предложением считать использование ИИ отягчающим обстоятельством в преступлениях. Помимо этого, «Справедливая Россия» занимается разработкой законопроектов о «госнейроконтроле» – решения ИИ будут обязательно проверяться человеком.

Деятельность ЛДПР в секторе ИИ по-прежнему ассоциируется преимущественно с проектом «Нейрожириновский» (2023 г.), хотя либерал-демократы и стремятся расширить «тематическую корзину» путем внесения законопроектов. В частности, уже несколько лет продвигают право использовать ИИ в предвыборной агитации, однако безуспешно.

КПРФ, изначально обвинявшая ИИ в «отсутствии духовности», осознает «тектонические сдвиги», которая несет в себе технология. При этом основное внимание партии сосредоточено на проблеме замещения человеческого труда роботами (к которым они относят и искусственный интеллект). Коммунисты верят: справиться с последствиями внедрения ИИ сможет только социалистическое государство, однако конкретных инициатив партия предлагать не торопится.

Заключение. В целом все парламентские партии сталкиваются с общим вызовом – стремительной трансформацией ИИ. Перемены происходят настолько часто, что законы не успевают за развитием «цифрового разума». Тем не менее, депутаты продолжают работу, в том числе на межфракционной основе. Так, например, по поручению председателя Госдумы Вячеслава Володина в нижней палате создана рабочая группа, в которую вошли депутаты от «Единой России», ЛДПР, «Справедливой России» и «Новых людей». Главная задача рабочей группы – «точечно регулировать отраслевые запросы», а также «вводить пилотные режимы» [1]. Ни парламентарии, ни правительство не спешат с ужесточением правил – учитывают риски того, что быстро введенные ограничения могут в перспективе навредить технологическому лидерству России в отрасли. Однако в долгосрочной перспективе успех и поддержка инициатив

парламентских партий в сфере ИИ во многом будут зависеть от умения совместно и своевременно синхронизироваться с глобальными трендами. И здесь важно «играть в долгую», делая ставку не на популистские и яркие инициативы, но на системное совершенствование нормативно-правовой базы.

Список источников и литературы:

1. В Госдуме появилась рабочая группа по регулированию ИИ [Электронный ресурс] // Forbes : сайт. 09.04.2025. URL: https://www.forbes.ru/tekhnologii/534665-v-gosdume-poavilas-rabocaa-gruppa-po-regulirovaniu-ii (дата обращения: 10.11.2025).

2. Горе от интеллекта. Использование ИИ отрегулируют законом [Электронный ресурс] // Коммерсантъ : сайт. 14.04.2023. URL: https://www.kommersant.ru/doc/5928661 (дата обращения: 10.11.2025).

3. «Единая Россия» представила «Цифровой манифест» партии [Электронный ресурс] // ТАСС : сайт. 17.08.2021. URL: https://tass.ru/ekonomika/12149831 (дата обращения: 10.11.2025).

4. «Мигрант ID»: в России предлагают создать цифровые профили иностранцев [Электронный ресурс] // ГТРК «Южный Урал» : сайт. 22.10.2025. URL: https://www.cheltv.ru/migrant-id-v-rossii-predlagayut-sozdat-tsifrovye-profili-inostrantsev/ (дата обращения: 10.11.2025).

5. Несколько агентств заинтересовались сотрудничеством с ИИ-актрисой Тилли Норвуд [Электронный ресурс] // Forbes : сайт. 29.09.2025. URL: https://www.forbes.ru/forbeslife/546821-neskol-ko-agentstv-zainteresovalis-sotrudnicestvom-s-ii-aktrisoj-tilli-norvud (дата обращения: 10.11.2025).

6. Сбербанк обогнал JPMorgan и впервые возглавил рейтинг мировых эквайеров [Электронный ресурс] // РБК : сайт. 17.10.2025. URL: https://www.rbc.ru/finances/17/10/2025/68f234499a7947075caddf7d (дата обращения: 10.11.2025).

7. Впервые в народной программе «Единой России» появится технологический блок — партия разработает его с сообществом инноваторов и учёных к выборам в Госдуму [Электронный ресурс] // «Единая Россия» : сайт. 30.09.2025. URL: https://er.ru/activity/news/vpervye-v-narodnoj-programme-edinoj-rossii-poyavitsya-tehnologicheskij-blok-partiya-razrabotaet-ego-s-soobshestvom-innovatorov-i-uchyonyh-k-vyboram-v-gosdumu (дата обращения: 10.11.2025).

Владислав Павлович Тищенко,
магистрант факультета иностранных языков ФГБОУ ВО «ВГПУ»,
E-mail: tishvladi@mail.ru

Мария Александровна Шевцова,
заведующий кафедрой английского языка ФГБОУ ВО «ВГПУ», доцент, кандидат педагогических наук

Vladislav P. Tishchenko
Master graduate, Faculty of Foreign Languages,
Voronezh State Pedagogical University
Email: tishvladi@mail.ru

Maria A. Shevtsova
Head of the English Language Department, Voronezh State Pedagogical University, Associate Professor, PhD in Pedagogical Sciences

СОЗДАНИЕ УЧЕБНОГО ПОСОБИЯ, НАПРАВЛЕННОГО НА РАЗВИТИЕ КОММУНИКАТИВНЫХ НАВЫКОВ НА ОСНОВЕ ОБРАЗОВАТЕЛЬНЫХ ЖУРНАЛОВ

CREATING A STUDENTS' BOOK AIMED AT DEVELOPING COMMUNICATION SKILLS BASED ON EDUCATIONAL MAGAZINES

Аннотация. Статья посвящена созданию учебного пособия, ориентированного на развитие коммуникативных навыков в изучении иностранных языков с использованием образовательных журналов, с примерами первого интерактивного образовательного российского журнала EnglishMag. Рассматриваются теоретические основы формирования коммуникативной компетенции, роль аутентичных и интерактивных материалов в процессе обучения, а также ключевые компоненты пособия, способствующие развитию всех видов речевой деятельности. Особое внимание уделяется современным методикам, адаптации материала по уровням владения языком и интеграции цифровых технологий. Приводится перечень актуальных образовательных журналов, полезных для создания эффективных учебных пособий.

Ключевые слова: создание учебного пособия, развитие коммуникативных навыков, образовательные журналы, EnglishMag, интерактивное обучение, аутентичные материалы, уровни владения языком, интерактивные задания.

Abstract. This article focuses on the creation of a textbook aimed at developing communicative skills in foreign language learning through the use of educational magazines, with the example of the first interactive educational Russian magazine EnglishMag. It covers the theoretical foundations of the communicative development approach, the role of authentic and interactive materials in the learning process, and key components of the textbook that promote the development of all types of speech activities. Special emphasis is placed on modern methodologies, adaptation of materials according to language proficiency levels, and the integration of digital technologies. A list of relevant educational magazines useful for creating effective textbooks is also provided.

Keywords: creating textbooks, developing communicative skills, educational magazines, EnglishMag, interactive learning, authentic materials, language proficiency levels, interactive tasks.

В условиях современного языкового образования особое внимание уделяется развитию коммуникативных навыков, которые являются ключевыми для успешного общения на иностранном языке. Л.С. Выготский считал, что первоначальной функцией речи является коммуникативная функция. В речевой деятельности он отмечал, прежде всего, средство социального общения, средство высказывания и понимания, следовательно, возможность социального становления человека и всех его познавательных сил [1]. Одним из эффективных инструментов для формирования этих навыков становятся учебные пособия, основанные на актуальных образовательных ресурсах, включая источники из средств массовой информации (СМИ), в том числе образовательные журналы. В этой статье рассматриваются основные составляющие компоненты по созданию учебного пособия с акцентом на коммуникативные навыки, используя материалы образовательных журналов. Особое внимание уделяется журналу EnglishMag, а также перечню актуальных образовательных и информационных изданий, способствующих развитию языковой компетенции.

Современные методики обучения иностранным языкам делают акцент на развитие информационно-коммуникационных технологий и коммуникативной компетенции как способности реализовывать эффективное речевое общение в различных ситуациях. Научные исследования подчеркивают необходимость личностно-ориентированного подхода и постепенного перехода от формального знания к реальным коммуникативным действиям, то есть к применению полученных умений на практике. Формирование коммуникативных умений требует системного использования разнообразных видов деятельности: говорение, аудирование, чтение и письмо, что позволяет комплексно развивать языковую практику [6; 7].

В данной ситуации, образовательные журналы выступают важным ресурсом, предоставляющим актуальные и контекстуализированные учебные материалы. Они могут служить источником аутентичных текстов, диалогов, упражнений. Кроме упомянутого выше, это могут быть диктофонные записи, сделанные во время интервью с носителями языка (американцами, британцами, канадцами, австралийцами) или с людьми, для которых английский – второй язык, но они его освоили до такого уровня, который позволяет свободно общаться на

различные темы, в том числе и профессиональные. И такие аудиозаписи интервью, конечно, способствуют развитию речевых навыков, так как являются живым примером использования английской лексики в реальных ситуациях. Журнал EnglishMag занимает особое место как первый интерактивный образовательный журнал в России, направленный на изучающих английский и русский как иностранный (за счёт создания статей с параллельным переводом (EN-RU) и выделением ключевых слов для уровня A2-B2). А возможность одновременного чтения и прослушивания статей выпусков EnglishMag способствует улучшению произношению, что значительно облегчает восприятие языка и помогает укреплять коммуникативные навыки [8][9].

Создание эффективного учебного пособия предполагает включение ряда компонентов, способствующих развитию умений общения:

– Использование интерактивных и настольных игр, например, «змейки» или морской бой, где нужно задать определенный вопрос, например, соответствующий по цвету и виду одежды. Все эти настольные игры стимулируют диалог и развивают совместную коммуникацию [5].

– Наличие интерактивных тестов для оценивания успешности обучения учащихся.

– Внедрение аутентичных материалов, приближенных к реальным жизненным ситуациям (интервью, истории реальных людей, видео-блоги о путешествиях по России иностранцев) с возможностью прослушать аудио к тексту на сайте.

– Наличие вокабуляра к статьям (делает статью удобной для понимания разному кругу читателей).

– Наличие интерактивной рабочей тетради с заданиями (нововведение появилось впервые в образовательном журнале EnglishMag в 2018 году, благодаря идее редактору Рамону Акоста, преподавателя английского языка, переехавшего в Россию на ПМЖ) [6].

– Применение интерактивных технологий (открытие страницы по QR-коду из журнала) и цифровых ресурсов для разнообразия методов обучения.

– Оценочное и регулярное тестирование (Placement and Review tests) и оценка коммуникативных успехов обучающихся с помощью открытых вопросов преподавателя ученику.

– Гибкая адаптация материала под различные уровни владения языком (A1-B2) и интересы учащихся.

Примеры образовательных журналов для создания учебного пособия

Для разработки пособия, ориентированного на развитие коммуникативных навыков, планируется рассмотреть использование материалов (при согласии авторов) из следующих образовательных журналов и порталов:

1. EnglishMag – интерактивный журнал с параллельными текстами на английском и русском языках с вопросами для обсуждений и рабочей тетрадью [3]. Доступность журнала в международных библиотеках в странах старого и нового света помогает достичь широкого круга читателей, которые интересуются Россией и хотели бы учить русский как иностранный [11].

2. Иностранные языки в школе – научно-методический журнал о теории и практике преподавания иностранных языков [4].

3. Russia Today (RT) – первый русский англоязычный новостной канал, который вещает новости 24/7 и показывает российскую точку зрения на глобальные новости. Медиапортал, охватывающий ТВ, радио, онлайн-вещание, и публикацию статей по разным актуальным тематикам, таким как международные отношения, политика, экономика, спорт и другие [12].

4. «Окно в Россию» (Gateway to Russia) – портал, на котором иностранцы могут выучить русский язык и получить всю нужную информацию перед путешествием в Россию, в том числе о том, как получить визу [10].

5. «Английский язык в школе» (English at school) – учебно-методический журнал, который издается с 2002 года и предназначен для учителей английского языка [2].

Заключение. Подводя итог, важно сказать, что учебное пособие на основе материалов образовательных журналов позволяет комплексно и эффективно развивать коммуникативные навыки, а также информационно-коммуникационной компетентности учащихся. Использование актуальных и интерактивных ресурсов, таких как EnglishMag, RT, Gateway to Russia, помогает сделать процесс обучения более интересным и продуктивным. Важным аспектом выступает интеграция современных информационно-коммуникационных технологий и разнообразных видов речевой деятельности, что способствует формированию полноценной языковой компетенции, необходимой для практического общения в реальной жизни.

Нужно отметить, что учебное пособие, построенное на базе современных образовательных журналов, становится мощным инструментом в арсенале методистов и преподавателей для достижения высоких и ускоренных результатов в обучении иностранным языкам, но требует также возможной доработки материала под конкретные случаи использования.

Список источников и литературы:

1. Александрова Н. С., Петушкова О. А. Ретроспективный анализ понятия коммуникативно-речевой активности дошкольников в психолого-педагогических исследованиях // Проблемы современного педагогического образования. 2020. №69-1. – URL: https://cyberleninka.ru/article/n/retrospektivnyy-analiz-ponyatiya-kommunikativno-rechevoy-aktivnosti-doshkolnikov-v-psihologo-pedagogicheskih-issledovaniyah (дата обращения: 10.11.2025).

2. Английский язык в школе (English at school). Издательство «Титул» – URL: https://titul.ru (дата обращения: 10.11.2025).

3. Архивные выпуски EnglishMag (2018-2022 годы) – URL: https://biblioclub.ru/index.php?page=journal_red&jid=686225 (дата обращения: 10.11. 2025).

4. Иностранные языки в школе – URL: https://iyash.ru/ (дата обращения: 10.11.2025).

5. Лихтарников Л.М. Занимательные логические задачи. СПб.: "Лань", 1996. – 124 с. – URL: https://djvu.online/file/tO4zVtJXODUr3 (дата обращения: 10.11.2025).

6. Методика формирования коммуникативных умений и навыков в профессиональной подготовке будущих учителей математики. / Османова И.М. - 2003. – URL: https://www.dissercat.com/content/metodika-formirovaniya-kommunikativnykh-umenii-i-navykov-v-professionalnoi-podgotovke-budush (дата обращения: 10.11.2025).

7. Методики развития коммуникативных навыков в процессе обучения английскому языку на начальном этапе. / Шайнурова Э.И. – URL: https://archive-coursework.mmu.ru/files/upload/Diplomas/2024/publish/p_8899_879.pdf (дата обращения: 10.11.2025).

8. Пример статьи с параллельным переводом – URL: https://englishmag.ru/englishman-in-voronezh (дата обращения: 10.11.2025).

9. Примеры записей с тренировкой навыков Listening – URL: https://vk.com/english_mag/listen (дата обращения: 10.11.2025).

10. EnglishMag 1Q/2022 – Malta Libraries. – URL: https://maltalibraries.overdrive.com/media/6629461 (дата обращения: 10.11.2025).

11. Gateway to Russia – URL: https://gw2ru.com (дата обращения: 10.11.2025).

12. RT – Breaking News, Russia News, World News and Video – URL: https://rt.com (дата обращения: 10.11.2025).

Матео Рохас Сампер,
Аспирант, Кафедра мировых политических процессов, Факультет управления и политики, Московский государственный институт международных отношений (МГИМО)ORCID: 0000-0002-1212-8146
E-mail: mrokhassamper@edu.hse.ru

Mateo Rojas Samper,
PhD student in the Department of World Politics at the Faculty of Governance and Politics, Moscow State Institute of International Relations (MGIMO).
ORCID: 0000-0002-1212-8146
E-mail: mrokhassamper@edu.hse.ru

МАГИЧЕСКИЙ РЕАЛИЗМ КАК МЕХАНИЗМ ЭПИСТЕМОЛОГИЧЕСКОГО СОПРОТИВЛЕНИЯ: ПЕРЕОСМЫСЛЕНИЕ ПОСТКОЛОНИАЛЬНОГО СУВЕРЕНИТЕТА В УСЛОВИЯХ ИКТ И ГЛОБАЛЬНОГО УПРАВЛЕНИЯ ИНТЕРНЕТОМ

MAGIC REALISM AS A MECHANISM OF EPISTEMOLOGICAL RESISTANCE: RETHINKING POST-COLONIAL SOVEREIGNTY IN THE CONTEXT OF ICT AND GLOBAL INTERNET GOVERNANCE

Аннотация. Данная работа посвящена исследованию магического реализма в литературе Колумбии и Мексики как мощного исторического механизма эпистемологического сопротивления против западноцентричных моделей знания, которые были навязаны в ходе колонизации и сохраняются в эпоху неоколониализма. Исследование доказывает, что этот уникальный латиноамериканский культурный феномен заложил фундаментальную основу для понимания современных вызовов, стоящих перед цифровым суверенитетом и информационной безопасностью стран Глобального Юга. Анализ фокусируется на том, как подрыв рациональности, характерный для магического реализма, предлагает готовую стратегическую модель для эффективного противодействия гегемонии в сферах информационно-коммуникационных технологий (ИКТ) и глобального управления Интернетом. Особое внимание уделяется глубокой концепции «колониальности знания» и ее трансформации в ее современное проявление «колониальность цифрового», подчеркивая, что борьба за цифровую автономию является прямым продолжением борьбы за культурную независимость, включая использование музыки как контрнарратива и анализ конкретных примеров культурного производства.

Ключевые слова: постколониализм; магический реализм; цифровой суверенитет; информационная безопасность; управление Интернетом; Латинская Америка; эпистемологическое сопротивление; колониальность знания; культурный суверенитет.

Abstract. This work investigates magical realism in the literature of Colombia and Mexico as a powerful historical mechanism of epistemological resistance against the Western-centric models of knowledge that were imposed during colonization and persist in the era of neo-colonialism. The study argues that this unique Latin American cultural phenomenon has laid a fundamental foundation for understanding the modern challenges facing the digital sovereignty and information security of countries in the Global South. The analysis focuses on how the subversion of rationality characteristic of magical realism offers a ready-made strategic model for effectively countering hegemony in the spheres of Information and Communication Technologies (ICT) and global Internet governance. Particular attention is paid to the profound concept of the "coloniality of knowledge" and its transformation into its contemporary manifestation, the "coloniality of the digital," emphasizing that the struggle for digital autonomy is a direct continuation of the struggle for cultural independence, including the use of music as a counter-narrative and the analysis of specific examples of cultural production.

Keywords: Post-colonialism; magical realism; digital sovereignty; information security; Internet governance; Latin America; epistemological resistance; coloniality of knowledge; cultural sovereignty.

Введение. Постколониальный вызов цифровой гегемонии и роль культуры в обеспечении безопасности. Современный международный дискурс, касающийся цифрового суверенитета и глобального управления Интернетом, имеет тенденцию концентрироваться исключительно на его технических, юридических и экономических аспектах, зачастую игнорируя исторический и культурный контекст. Для стран Латинской Америки и Глобального Юга, в целом, эти вопросы неотделимы от истории колониального и неоколониального доминирования, которое оставило глубокий след не только в политических институтах, но и в самой структуре знания [8]. В настоящей работе предлагается критический взгляд на проблему цифрового суверенитета, рассматривая его не как техническую необходимость, а как прямое продолжение и современное проявление культурного суверенитета. Мы исследуем, каким образом механизмы эпистемологического сопротивления, выработанные латиноамериканской культурой в постколониальный период, могут быть непосредственно применены для информирования и укрепления национальных стратегий информационной безопасности в условиях растущего технологического дефицита и гегемонии данных. Центральный вопрос, который мы ставим, заключается в следующем: каким образом культурное производство, подрывающее общепринятую западную рациональность, может создать необходимую основу для

формирования суверенного цифрового мировоззрения, которое способно противостоять новым формам внешнего контроля и гегемонии в информационной сфере?

Теоретические рамки. Деколониальный поворот и множественность суверенитетов. Данное исследование опирается на фундаментальные положения постколониальной теории, развитой такими мыслителями, как Эдвард Саид и Хоми Бхабха, и, особенно, на концепции деколониального поворота, представленные Анибалом Кихано и Вальтером Миньоло. В рамках этого подхода суверенитет интерпретируется не только как фиксированный юридический факт, основанный на Вестфальской модели, но, прежде всего, как динамический социально-культурный конструкт [2], который постоянно оспаривается и переопределяется. Для постколониальных государств региона достижение политической независимости не ознаменовало автоматического конца «колониальности власти» и, что более важно для нашего анализа, «колониальности знания». Последняя выражалась в навязывании европейской философии, историографии, а также системы ценностей и классификации в качестве единственно универсальной, объективной и научной. Ученые, такие как Санджай Сет, убедительно продемонстрировали, что сама структура социальных наук и рационального мышления, принятая в академическом мире, глубоко укоренена в европейском Просвещении и служит для маргинализации незападных способов познания.

Магический реализм как акт суверенного утверждения и анти-историография. Магический реализм стал ключевым инструментом противодействия этому навязыванию. В отличие от европейского сюрреализма, который часто искал фантастическое в сфере подсознания или мечты, латиноамериканский магический реализм, представленный такими авторами как Габриэль Гарсиа Маркес («Сто лет одиночества») и Хуан Рульфо («Педро Парамо»), находил магическое и иррациональное в самой повседневной латиноамериканской реальности [5]. Путем радикального смешения мифа, истории, фольклора и обыденности, магический реализм достигал нескольких ключевых целей: во-первых, он выступал как анти-историография, создавая альтернативную, циклическую или многослойную историю, которая восстанавливала индигенную и национальную память, стертую или искаженную линейной колониальной историографией. В «Стах лет одиночества» временная петля и фантастические события служат метафорой для трагического и абсурдного цикла неоколониальной зависимости. Во-вторых, он утверждал множественные истины и формы знания, бросая прямой вызов монополии западной науки на объективность, эмпиризм и единственную рациональность. Следовательно, магический реализм – это не просто литературный прием, а мощный акт суверенного утверждения права на собственное, неевропейское миропонимание, которое является абсолютно необходимой

предпосылкой для достижения подлинной и полной независимости. Этот механизм сопротивления лежит в основе нашего тезиса о цифровом суверенитете.

Музыка и литература как контрнарративы: кейс-стади Колумбии и Мексики. Анализ не ограничивается только литературой. Музыка также функционирует как звуковой контрнарратив. Музыкальные жанры, отражающие борьбу за гражданские права и идентичность (например, мексиканские корридос или колумбийская кумбия в ее социальных проявлениях), исторически обходили цензуру и идеологические барьеры, проникая в общественное сознание и укрепляя коллективную память о сопротивлении. Они представляют собой форму «устной истории», которая часто противоречит официальной, евроцентричной версии событий. В цифровую эпоху эти контрнарративы сталкиваются с новой проблемой –технологической гомогенизацией. Когда глобальные платформы для стриминга и социальные сети диктуют, что является «популярным» или «релевантным» через алгоритмическую фильтрацию и рекомендации, они невольно (или намеренно) маргинализируют местные культурные формы, которые не соответствуют их глобализированной, коммерческой логике. Таким образом, борьба за суверенитет в сфере ИКТ становится борьбой за право быть услышанным и за сохранение культурной сложности вне рамок, заданных глобальными медиагигантами. Наш кейс-стади Колумбии и Мексики демонстрирует, как их богатое культурное производство служит лабораторией для выработки устойчивости против этой цифровой унификации.

Трансформация «колониальности знания» в «колониальность цифровую» и риски ИИ. Мы утверждаем, что сегодняшние вызовы в сфере ИКТ и управления Интернетом являются прямым следствием трансформации «колониальности знания» в «колониальность цифровую». Это проявляется в нескольких измерениях, критически важных для международной информационной безопасности. Интернет остается под контролем западных корпораций, что ведет к ограничению цифрового суверенитета стран Латинской Америки. Зависимость от иностранных облачных сервисов, стандартов и протоколов ограничивает способность государств управлять своими информационными потоками, что представляет прямую угрозу информационной безопасности и устойчивости критической инфраструктуры. Системы искусственного интеллекта (ИИ), которые все чаще используются в принятии решений, обучены преимущественно на данных, сформированных в западном контексте. Это неизбежно воспроизводит и закрепляет скрытое алгоритмическое смещение (bias)[12]. Это смещение не просто техническая ошибка; это эпистемологическая ошибка, которая может закрепить исторические социальные, расовые или экономические предубеждения, игнорируя уникальные, нелинейные, «магически-реалистические» паттерны социальной жизни Латинской Америки. Следовательно, доверие к таким системам подрывает национальный суверенитет над данными и знаниями. Модели

управления, продвигаемые G7 и другими западными акторами, часто не учитывают или недооценивают суверенные интересы Глобального Юга. Необходимость суверенного контроля над данными (цифровой суверенитет) является реакцией на эту гегемонию, а не просто желанием изоляции.

Модель суверенного ответа: интеграция культурной автономии в цифровую стратегию. Опыт магического реализма предлагает готовую модель для выработки устойчивых стратегий в ответ на вызовы цифровой колониальности. Он учит, что утверждение суверенитета заключается не в изоляции, а в способности трансформировать входящие культурные и технологические потоки, инкорпорируя их в собственную сложную и многослойную реальность. Национальные стратегии должны требовать эпистемологической диверсификации в разработке ИИ. Это означает инвестиции в создание местных наборов данных, которые отражают уникальные социальные и культурные реалии, включая нелинейное, мифологическое и индигенное знание. Это необходимо для снижения алгоритмического смещения и укрепления информационной безопасности. Латиноамериканские государства должны настаивать на том, что цифровой суверенитет включает право на защиту локального контента и языков. Их голос в структурах глобального управления Интернетом (например, IGF) должен быть направлен на установление норм, которые признают культурную автономию как основу цифровой безопасности.

Использование культурного производства для киберустойчивости: Культурное производство, перешедшее в цифровую сферу, должно активно использоваться не только для развлечения, но и для укрепления гражданского сознания и киберустойчивости, создавая контрнарративы против дезинформации и внешнего идеологического влияния, используя тот же самый «гибридный» язык, которым пользовался магический реализм для борьбы с колониализмом.

Заключение. Подводя итог, следует констатировать, что стремление к цифровому суверенитету в постколониальных государствах, таких как Колумбия и Мексика, не может быть сведено к простому набору технических мер или юридических рамок, навязанных извне. Достижение истинной автономии требует, прежде всего, эпистемологической деколонизации, то есть критического пересмотра и отказа от парадигм знания, которые продолжают воспроизводить иерархии власти, заложенные колониальной эпохой. Наш анализ показывает, что магический реализм в литературе и музыке Латинской Америки выступает не просто как художественный жанр, а как исторический, проверенный временем пример успешного культурного сопротивления. Он убедительно продемонстрировал, как можно отстоять право на собственное, отличное от западного, мировоззрение, путем легитимизации альтернативных форм знания и восприятия времени и пространства.

Перенос этого глубокого культурного опыта в сферу ИКТ, кибербезопасности и глобального управления Интернетом является не просто академическим упражнением, но ключевым стратегическим императивом для стран Глобального Юга. Борьба за суверенную архитектуру Интернета, за непредвзятость алгоритмов ИИ и за сохранение локальных цифровых идентичностей это, по сути, та же самая борьба за право на самоопределение, которую вели писатели и музыканты прошлого века. Мы не можем ожидать, что технологические решения, разработанные в рамках доминирующей рациональности, автоматически послужат интересам деколонизации. Напротив, они часто являются новыми каналами для старой гегемонии. Следовательно, культурная автономия, которая веками защищалась искусством от романов Гарсиа Маркеса до песен протеста должна быть интегрирована как неотъемлемая часть стратегического обеспечения информационной безопасности в XXI веке. Только через признание и активное внедрение своего уникального, гибридного и нелинейного способа познания (того, что мы назвали «магически-реалистичным подходом») эти нации смогут построить справедливую, безопасную и по-настоящему суверенную цифровую архитектуру будущего, свободную от неявных форм цифрового колониализма. Это требует от политиков и технологов смелости мыслить за пределами стандартных моделей безопасности, признавая, что культурный код нации является ее самой надежной линией обороны в информационной войне идей.

Список источников и литературы:

1. Бхабха Х. К. Местонахождение культуры / Пер. с англ. М.: Ad Marginem, 2014. 352 с.
2. Вендт А. Социальная теория международной политики / Пер. с англ. М.: РОССПЭН, 2018. 496 с.
3. Дердериан Дж. Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network. Cambridge: MIT Press, 2009. 336 p.
4. Кихано А. Колониальность власти, европоцентризм и Латинская Америка // Деколонизация. Политика и культура в Латинской Америке. М.: ИМЭМО РАН, 2019. С. 88-145.
5. Маркес Г.Г. Сто лет одиночества. М.: АСТ, 2020. 480 с.
6. Миньоло В. У. Идея Латинской Америки: Колониальность, суверенитет и деколониальный поворот. М.: Новое литературное обозрение, 2021. 248 с.
7. Моргентау Г. Дж. Политические отношения между нациями: Борьба за власть и мир. М.: Идея-Пресс, 2017. 592 с.
8. Саид Э. В. Ориентализм. Западные концепции Востока / Пер. с англ. СПб.: Русский міръ, 2006. 640 с.

9. Сети С. Beyond Reason: Postcolonial Theory and the Social Sciences. New Haven: Yale University Press, 2019. 304 p.
10. Фанон Ф. Черная кожа, белые маски. М.: Ad Marginem, 2020. 288 с.
11. Hardt M., Negri A. Empire. Cambridge: Harvard University Press, 2000. 480 p.
12. Walker R. B. J. Inside/Outside: International Relations as Political Theory. Cambridge: Cambridge University Press, 1993. 240 p.

Николай Дмитриевич Герасимов,
аспирант кафедры всеобщей истории, политологии и регионоведения
ФГБОУ ВО «МГУ им. Н. П. Огарёва»
E-mail: nickogerasimov@vk.com

Nikolai D. Gerasimov,
Postgraduate student of the Department
of General History, Political Science and Regional Studies
of the Mordovian State University
E-mail: nickogerasimov@vk.com

ВИЗУАЛИЗАЦИЯ АКТУАЛЬНОЙ ВНЕШНЕПОЛИТИЧЕСКОЙ ПРОБЛЕМАТИКИ РОССИЙСКИМИ ПАРТИЯМИ

VISUALIZATION OF CURRENT FOREIGN POLICY ISSUES BY RUSSIAN PARTIES

Аннотация. В статье анализируется визуализация актуальной внешнеполитической проблематики в коммуникационных стратегиях российских партий «Единая Россия» и «Новые люди» на примере их Telegram-каналов за октябрь 2025 года. Методами количественного и качественного контент-анализа, а также оценки метрик вовлеченности выявлено, что, несмотря на малый объем контента, внешнеполитическая тематика выполняет ключевые идеологические функции. «Единая Россия» использует конструктивно-союзнический и конфронтационно-критический нарративы, в то время как «Новые люди» фокусируются на теме цифрового суверенитета, что находит высокий отклик у их аудитории.

Ключевые слова: визуальные технологии, визуальный политический дискурс, внешнеполитическая проблематика, политические партии России, коммуникационные стратегии, социальные сети.

Abstract. The article analyzes the visualization of current foreign policy issues in the communication strategies of the Russian parties «United Russia» and «New People» using the example of their Telegram channels for October 2025. Using methods of quantitative and qualitative content analysis, as well as assessment of engagement metrics, it was revealed that, despite the small volume of content, foreign policy issues perform key ideological functions. United Russia uses constructive-allied and confrontationally critical narratives, while New People focuses on the topic of digital sovereignty, which finds a high response from their audience.

Key words: visual technologies, visual political discourse, foreign policy issues, political parties of Russia, communication strategies, social networks.

Визуализация в политической коммуникации. Современная политическая коммуникация в 2025 году активно использует визуальные средства как ключевой инструмент трансляции партийных идеологий и внешнеполитических позиций [3]. Визуализация в российском политическом дискурсе представляет собой не просто контент, а систему символов и образов, формирующих восприятие международных процессов и места России в мире.

Исследования показывают, что визуальные форматы от фотографий до инфографики служат не только средством передачи информации, но и создают эмоциональный отклик и идеологическую идентичность [4]. Особенно значимой визуальная риторика становится в периоды внешнеполитических кризисов, когда рождается спрос на визуальные образы с целью снижения психологического диссонанса и созданию психологической защиты потребителя контента. В более же спокойные периоды акцент смещается на образы стабильности, благополучия и национального единства. Рассмотрим это на конкретных примерах.

Визуализация внешнеполитической проблематики «Единой Россией». Анализ данных проводился на основе массива публикаций официального канала партии «Единая Россия» в мессенджере Telegram за октябрь 2025 года [1]. Общий объем проанализированного контента составил 183 публикации. Для решения исследовательских задач был применен комплекс методов, включая количественный и качественный контент-анализ, а также статистический анализ метрик вовлеченности аудитории.

Количественный анализ тематической структуры контента. В результате количественного анализа было установлено, что из всего массива публикаций лишь 11 сообщений были целиком посвящены внешнеполитической тематике. В процентном соотношении это составляет примерно 6 % от общего объема контента. Данное распределение демонстрирует, что внешняя политика не является доминирующим тематическим направлением в коммуникационной стратегии партии в рассматриваемый период. Основной фокус внимания сосредоточен на внутренней повестке, включая поддержку участников Специальной военной операции (СВО), реализацию «Народной программы» и освещение социально-экономического развития регионов.

Качественный анализ позволил выявить два ключевых нарратива, формирующих внешнеполитический дискурс партии.

Первый нарратив можно охарактеризовать как конструктивно-союзнический. Он был репрезентирован в рамках освещения официального визита делегации «Единой России» в КНДР [1]. В соответствующих сообщениях акцент делался на стратегическом характере двусторонних

отношений, взаимной поддержке на международной арене и общности подходов к формированию многополярной архитектуры мира. Тон публикаций был выдержан в позитивном ключе и подчеркивал поступательное развитие диалога.

Второй, конфронтационно-критический нарратив, занимал более существенное место в объеме внешнеполитического контента. Данный нарратив был направлен на критику действий США и их союзников, которые описывались через призму враждебности по отношению к России. В сообщениях, часто представлявших собой цитаты председателя партии Д.А.Медведева, использовалась более жесткая лексика [1].

Анализ вовлеченности аудитории. Для оценки резонанса внешнеполитических сообщений у аудитории были рассчитаны агрегированные метрики вовлеченности. Средние показатели для публикаций внешнеполитической направленности составили:

1) ER View (уровень вовлеченности от просмотров): примерно 2,15 % (пределы среднего уровня вовлечённости). ER View показывает, насколько аудитория вовлечена в контент (отношение взаимодействий к просмотрам). Чем выше процент, тем активнее аудитория реагирует на публикации.

2) VR Post (коэффициент виральности): примерно 22,5 (высокий показатель). VR Post отражает способность контента распространяться самостоятельно, без дополнительных усилий со стороны автора или сообщества. Чем выше коэффициент, тем лучше контент «расходится» среди пользователей.

Сравнительный анализ данных показателей с общими тенденциями канала показал, что они являются сопоставимыми или слегка повышенными. Наибольший отклик генерировали сообщения, содержащие прямую критику западных стран, а также репортажные публикации о значимых дипломатических событиях. Это свидетельствует о востребованности внешнеполитической тематики у целевой аудитории. Вместе с тем, абсолютный максимум виральности был зафиксирован у постов, посвященных поддержке участников СВО и их семей, что указывает на более высокий приоритет именно внутренней военной и социальной повестки для аудитории.

Таким образом, проведенный анализ данных позволяет констатировать, что, несмотря на ограниченный объем, внешнеполитическая тематика является органичной и значимой частью коммуникационной стратегии «Единой России», выполняя важные идеологические функции.

Визуализация внешнеполитической проблематики политической партией «Новые люди». Анализ данных публикационной активности партии «Новые люди» в октябре 2025 года проводился на основе массива из 33 публикаций их официального канала в мессенджере Telegram [2]. Для обеспечения сопоставимости результатов использовалась единая с

предыдущим исследованием методология, включающая количественный и качественный контент-анализ, а также расчет метрик вовлеченности аудитории. Результаты количественного анализа демонстрируют выраженную тематическую специализацию партии «Новые люди». Абсолютное большинство публикаций (31 из 33) были посвящены вопросам внутренней политики и социально-экономического развития. На внешнеполитическую тематику напрямую указывают лишь 2 публикации, что составляет 6,1% от общего объема контента. Данное распределение подтверждает фокус партии на внутренней проблематике, однако доля внешнеполитических сообщений незначительно, но превышает аналогичный показатель у «Единой России».

Качественный анализ двух идентифицированных внешнеполитических сообщений позволил выявить специфическую риторическую стратегию:

Во-первых, критический нарратив, направленный на Запад. Ключевая публикация от 21.10.2025 [2], посвященная дню рождения Павла Дурова, содержит критику регулирования интернета в странах ЕС (Германия, Великобритания) и Еврокомиссии. Партия использует эту тему для позиционирования себя как защитника цифровых свобод, проводя параллели с ограничениями в России («Все помнят закон о запрете ВПН»). Нарратив выстроен вокруг оппозиции «свобода vs. контроль» и использует эмоционально окрашенную лексику («цифровой концлагерь»).

Во-вторых, нарратив национальной идентичности. Публикация от 22.10.2025 [2], формально посвященная теме любви к Родине и традиционной русской одежде, содержит цитату Президента РФ о консолидации общества. Хотя прямо внешняя политика не обсуждается, этот пост можно рассматривать как косвенное участие в формировании государственного патриотического дискурса.

Расчет метрик вовлеченности для внешнеполитических публикаций показал следующие результаты:

1) ER View (уровень вовлеченности от просмотров): примерно 11,18 %;

2) VR Post (коэффициент виральности): примерно 41,8.

Сравнительный анализ выявил исключительно высокие показатели. Публикация о цифровой свободе от 21.10.2025 [2] продемонстрировала рекордные для всего исследуемого массива данных значения, что превышает не только средние показатели по каналу «Новые люди», но и максимальные значения вовлеченности, зафиксированные у «Единой России». Тема цифрового суверенитета и критики зарубежных практик вызвала активную дискуссию (335 комментариев), что указывает на ее высокую релевантность для аудитории партии.

Таким образом, анализ данных позволяет констатировать, что внешнеполитическая тематика является маргинальной по объему, но стратегически важной по воздействию в коммуникации партии «Новые люди». Партия использует ее для формирования образа современной, технологически ориентированной политической силы, отстаивающей права и свободы граждан в цифровую эпоху, что находит чрезвычайно высокий отклик у их целевой аудитории.

Заключение. Проведённый анализ позволяет сделать вывод о различных подходах партий «Единая Россия» и «Новые люди» к визуализации внешнеполитической проблематики. Если первая актуализирует традиционные дипломатические и силовые нарративы в рамках общегосударственной линии, то вторая избирательно использует тему цифрового суверенитета для формирования уникального имиджа, привлечения сторонников и консолидации своей электоральной базы. Отметим, что исследованные материалы позволяют идентифицировать лишь определённый срез проблемы, поскольку охватывают краткий временной период – один месяц. Такой подход обоснован обеспечением глубины и детализации исследования контента и метрик вовлеченности в конкретный момент времени, что, однако, не отменяет необходимости более масштабных исследований в будущем для выявления устойчивых тенденций.

Список источников и литературы:

1. Единая Россия. Официально [Электронный ресурс] // Телеграм-канал. – URL : https://t.me/s/er_molnia (дата обращения : 11.11.2025).

2. Партия «Новые люди» [Электронный ресурс] // Телеграм-канал. – URL : https://t.me/s/partynewpeople (дата обращения: 11.11.2025).

3. Скорик А.В. Визуализация как политическая технология // Вестник Российского университета дружбы народов. Серия: Политология. – 2018. – Т. 20. – № 4. – С. 609-615.

4. Bleiker R. Visualizing international relations: Challenges and opportunities in an emerging research field // Journal of Visual Political Communication. – Volume 10. – Issue 1. – Apr 2023. – P. 17-25.

Александра Ильинична Соловьева,
студент 1 курса магистратуры
направления Международные отношения,
программа «Дипломатия и современная дипломатическая система»,
Дипломатическая академия МИД России,
E-mail: alexspringsol@yandex.ru

Alexandra I. Solovyeva,
1st-year Master's student,
"Diplomacy and the Modern Diplomatic System,"
International Relations,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
E-mail: alexspringsol@yandex.ru

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СМИ В УСЛОВИЯХ ПЛАТФОРМЕННОЙ МЕДИАСРЕДЫ

DIGITAL TRANSFORMATION OF THE MEDIA IN A PLATFORM-BASED MEDIA ENVIRONMENT

Аннотация. В статье анализируются структурные изменения глобальной медиасреды в условиях перехода к платформенной модели распространения информации. Исследование демонстрирует, что ключевым объектом информационной безопасности становится не столько контент, сколько модель дистрибуции, контролируемая цифровыми платформами и алгоритмами рекомендаций. Рассматриваются теоретические модели массовой коммуникации в контексте их ограниченности в эпоху алгоритмического посредничества. Обозначены риски алгоритмической непрозрачности, технологической зависимости и международного давления на российские медиа. Проанализирована нормативно-правовая база в области регулирования рекомендательных технологий. Выделены стратегические перспективы развития медиасуверенитета и международной кооперации в сфере информационной безопасности.

Ключевые слова: информационная безопасность, цифровые платформы, рекомендательные алгоритмы, медиасуверенитет, международная информационная безопасность.

Abstract. The article examines structural changes in the global media environment driven by the transition to a platform-based model of information distribution. The study shows that the key object of information security today is not the content itself, but the distribution architecture controlled by digital platforms and recommendation algorithms. Classical models of mass communication are reconsidered in the context of their limitations in the era of algorithmic mediation. The article highlights the risks of

algorithmic opacity, technological dependence, and international political pressure on Russian media. It also analyses the regulatory framework governing recommendation technologies. The study outlines strategic perspectives for strengthening Russia's media sovereignty and for expanding international cooperation in the field of information security.

Keywords: information security, digital platforms, recommendation algorithms, media sovereignty, international information security.

Роль СМИ в современной архитектуре международной информационной безопасности. Современное медиапространство переживает радикальную перестройку, сопоставимую по масштабу с появлением телевидения в XX веке [1]. Если ранее коммуникация определялась логикой редакций, то теперь ключевым фактором становятся цифровые платформы, управляющие потоками информации через алгоритмы рекомендаций [1;2].

Несмотря на стремительное развитие искусственного интеллекта, информационных технологий и цифровой дипломатии, внимание к самим медиа часто оказывается вторичным. Однако именно СМИ формируют международные нарративы, влияют на восприятие государств [3]. Поэтому включение медиасреды в центр дискуссий об информационной безопасности и внешней политике становится ключевым сюжетом для понимания того, как реально формируется информационная повестка, транслирующая образ государств как во внутреннем периметре, так и на мировой арене [1;3].

Цифровая медиасреда: переход к платформенной модели. Данные российских и иностранных исследований показывают, что более половины пользователей получают новости от платформенных посредников – соцсетей, агрегаторов, видеохостингов [2;4;5]. Алгоритмы, а не редакции, определяют, какие темы становятся видимыми, а какие исчезают с радаров публичной сферы. Эта трансформация создаёт три фундаментальных сдвига:

- Алгоритм определяет и формирует структуру новостной ленты, индивидуальные информационные траектории пользователей [1;7].
- Роль традиционных каналов СМИ ослабляется –платформы контролируют каналы дистрибуции, метрики, монетизацию.
- Угроза информационного суверенитета усиливается, поскольку критические медиапроцессы оказываются в иностранной юрисдикции [7;8].

Эти изменения подводят нас к переосмыслению классических теорий коммуникации.

Теоретическая рамка: пересмотр модели Малецке в эпоху алгоритмов. Модель Малецке (1963 г.) рассматривала массовую коммуникацию как систему влияний –личностных, институциональных, социальных [10]. Журналист создаёт сообщение под давлением редакционной политики, профессиональных норм и образа аудитории.

Однако сегодня между коммуникатором и аудиторией появляется новый актор – платформа, которая:

- конструирует поведенческий профиль пользователя,
- решает, что достойно показа,
- формирует индивидуальное информационное поле.

Таким образом, платформа превращается в самостоятельный субъект коммуникации, а алгоритм –в механизм реализации информационной власти. Это требует расширения теоретических моделей за счёт включения алгоритмического посредничества как критического элемента информационной безопасности.

Риски платформенной зависимости для России. Прежде всего, это технологическая зависимость: до 2022 года более 80% видеопотребления приходилось на YouTube, а до половины поисковых запросов – на Google, что фактически означало концентрацию критических медиапотоков в иностранных юрисдикциях [9;15;16]. Дополнительно ситуацию осложняет алгоритмическая непрозрачность: платформы не раскрывают механизмов ранжирования, а значит, сохраняется высокая вероятность скрытой дискриминации российских источников и целенаправленного ограничения их видимости в информационных лентах [17;18].

К этому добавляются политические ограничения: в 2022–2024 годах блокировки и ограничения в отношении российских СМИ на западных платформах приобрели системный характер и привели к потере части международной аудитории [8;10].

Эти риски напрямую коррелируют с задачами Доктрины информационной безопасности РФ по обеспечению устойчивого и безопасного функционирования национальной информационной инфраструктуры.

Доктрина информационной безопасности РФ и новая медиасреда. Доктрина информационной безопасности РФ 2000 года рассматривала интернет прежде всего как объект, требующий техническую защиту: основной акцент делался на устойчивости сетей связи и критической инфраструктуры [12]. То есть защищалась прежде всего сама техническая инфраструктура, по которой распространялась информация. Доктрина 2016 года зафиксировала следующий уровень – содержательный: помимо инфраструктуры в фокус попали информационное и психологическое воздействие, защита суверенитета России в информационном пространстве, недопущение дискриминации российских СМИ за рубежом и формирование безопасной информационной среды для граждан [11]. С появлением платформенной медиасреды и алгоритмов рекомендаций возникает третий уровень повестки:

объектом безопасности становится уже система распространения контента, контролируемая цифровыми посредниками. От доктрины это требует перехода от защиты инфраструктуры и контроля содержания к регулированию самих механизмов дистрибуции – цифровых платформ, рекомендательных технологий и их прозрачности, а также к целенаправленному укреплению отечественных цифровых платформ [14;19].

Регулирование рекомендательных технологий в РФ. С 2023 года Россия развивает полноценную систему регулирования алгоритмов:

- ст. 10.2-2 149-ФЗ вводит требования к раскрытию правил работы рекомендаций [14;15];
- приказы РКН № 149 и № 150 (2023) определяют структуру «Правил применения рекомендательных алгоритмов» [16;17];
- ФЗ-530 закрепляет обязанности платформ по удалению запрещённого контента.

Российская модель сближается с глобальными тенденциями, в частности, с Digital Services Act ЕС, однако делает больший акцент на защите информационного суверенитета.

Стратегические перспективы медиасуверенитета России. Анализ позволяет выделить несколько ключевых стратегических направлений медиасуверенитета России. Во-первых, это развитие отечественных платформ – VK, RuTube, экосистемы «Яндекса» и других сервисов, которые обеспечивают устойчивость коммуникаций и снижают зависимость от иностранных инфраструктур. Во-вторых, регулирование алгоритмической архитектуры: создание механизмов, исключающих дискриминацию российских источников, и установление требований к прозрачности работы рекомендательных систем. Важным элементом становится и маркировка ИИ-контента вместе с более широким набором инструментов, ориентированных на укрепление доверия аудитории к национальной медиасреде.

Заключение. Цифровая трансформация СМИ радикально меняет представление о том, что такое информационная безопасность. Сегодня важна не только защита контента, но и контроль над системой распространения информации, находящейся в руках платформ и алгоритмов.

Для России стратегической задачей становится формирование устойчивой, суверенной медиасреды, способной противостоять внешним информационным воздействиям и эффективно продвигать российские позиции в международных отношениях.

Список источников и литературы:

1. Van Dijck J., Poell T., de Waal M. The Platform Society: Public Values in a Connective World [Электронный ресурс]. – Oxford: Oxford University Press, 2018. – Режим доступа: https://academic.oup.com/book/12378 (дата обращения: 30.11.2025).

2. Digital News Report 2024 [Электронный ресурс] // Reuters Institute for the Study of Journalism. – 2024. – Режим доступа: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024 (дата обращения: 30.11.2025).

3. Nye J. Soft Power: The Means to Success in World Politics [Электронный ресурс]. – New York: PublicAffairs, 2004. – Режим доступа: https://www.almendron.com/tribuna/wp-content/uploads/2020/02/joseph-s-nye-jr-soft-power.pdf (дата обращения: 30.11.2025).

4. Mediascope. Video Landscape и другие отчёты по онлайн-видеопотреблению в России в 2021–2022 гг. [Электронный ресурс]. – Mediascope, 2022. – Режим доступа: https://mediascope.ru (дата обращения: 30.11.2025).

5. Digital News Report 2023–2024: Country and Market Data [Электронный ресурс] // Reuters Institute for the Study of Journalism. – 2023–2024. – Режим доступа: https://reutersinstitute.politics.ox.ac.uk/digital-news-project (дата обращения: 30.11.2025).

6. Maletzke G. Psychologie der Massenkommunikation [Электронный ресурс]. – Hamburg: Hans-Bredow-Institut, 1963. Режим доступа: https://openlibrary.org/books/OL5671137M/Psychologie_der_Massenkommunikation (дата обращения: 30.11.2025).

7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [Электронный ресурс] // EUR-Lex. – 2022. – Режим доступа: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата обращения: 30.11.2025).

8. European Council. Decisions concerning restrictive measures in respect of Russian media outlets RT and Sputnik (2022–2024) [Электронный ресурс] // Official Journal of the European Union. – Режим доступа: https://www.consilium.europa.eu (дата обращения: 30.11.2025).

9. Mediascope Video Landscape 2021: ключевые показатели видеопотребления в России [Электронный ресурс]. – Mediascope, 2021. – Режим доступа: https://mediascope.ru (дата обращения: 30.11.2025).

10. ASD. Russia Media Monitoring 2023–2024 [Электронный ресурс] // Alliance for Securing Democracy. – 2024. – Режим доступа: https://securingdemocracy.gmfus.org (дата обращения: 30.11.2025).

11. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646 [Электронный ресурс] // Официальный интернет-портал правовой информации. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения: 30.11.2025).

12. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 09.09.2000 № 1300 [Электронный ресурс] // Президент России. – Режим доступа: http://kremlin.ru/acts/bank/15914 (дата обращения: 30.11.2025).

13. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Официальный интернет-портал правовой информации. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 30.11.2025).

14. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., включая ст. 10.2-2) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.11.2025).

15. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. 2023 г.), вводящий регулирование рекомендательных технологий [Электронный ресурс] // Официальный интернет-портал правовой информации. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 30.11.2025).

16. Приказ Роскомнадзора от 06.10.2023 № 149 «Об утверждении требований к содержанию информации о применении информационных технологий…» [Электронный ресурс] // Роскомнадзор. – Режим доступа: https://normativ.kontur.ru/document?moduleId=1&documentId=460885 (дата обращения: 30.11.2025).

17. Приказ Роскомнадзора от 06.10.2023 № 150 «Об утверждении формы уведомления о применении рекомендательных технологий…» [Электронный ресурс] // Роскомнадзор. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/408008917/ (дата обращения: 30.11.2025).

18. Федеральный закон от 30.12.2020 № 530-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”» (о правовом режиме социальных сетей) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_372264/ (дата обращения: 30.11.2025).

Екатерина Александровна Егорова,
студент 1 курса магистратуры факультета мировой политики,
Московский государственный университет им. М.В. Ломоносова
E-mail: kovalevak687@mail.ru

Ekaterina A. Egorova,
First-year Master's student at School of World Politics
Lomonosov Moscow State University
E-mail: kovalevak687@mail.ru

РОЛЬ АМЕРИКАНСКИХ СМИ КАК ИНСТРУМЕНТА ИНФОРМАЦИОННОЙ ВОЙНЫ США ПРОТИВ РОССИИ (НА МАТЕРИАЛЕ ИНОАГЕНТНОЙ МЕДИАКОМПАНИИ VOICE OF AMERICA)

THE ROLE OF AMERICAN MEDIA AS A TOOL OF US INFORMATION WARFARE AGAINST RUSSIAN TERRITORY (A CASE STUDY OF THE FOREIGN-AGENT MEDIA COMPANY VOICE OF AMERICA)

Аннотация. В статье проводится комплексный анализ роли американских средств массовой информации как инструмента информационной войны против Российской Федерации в период с 2014 по 2025 год на основе материалов американской международной общественной радиокампании, Voice of America. В фокусе внимания – стратегии, нарративы и методы, используемые данным медиаресурсом для воздействия на общественное сознание и политические процессы в Российской Федерации в период обострения международной обстановки. Особое внимание также уделяется теоретическим основам информационного противоборства, историческому контексту активизации деятельности западных медиа, а также конкретным направлениям их работы по формированию общественного мнения и поддержке определённых политических позиций.

Ключевые слова: информационная война, американские СМИ, информационная безопасность, гибридные войны, медиавоздействие, пропаганда, дезинформация, иноагенты, медиадискурс, манипулятивные технологии.

Abstract. The article provides a comprehensive analysis of the role of American mass media as a tool of information warfare against the Russian Federation from 2014 to 2025, based on materials from the US international public broadcasting network, Voice of America. The focus is on the strategies, narratives, and methods used by this media resource to influence public consciousness and political processes in the Russian Federation during a period of heightened international tensions. Particular attention is also paid to the theoretical foundations of information confrontation, the historical context

of the intensification of Western media activities, and the specific directions of their work in shaping public opinion and supporting certain political positions.

Keywords: information warfare, American mass media, information security, hybrid wars, media influence, propaganda, disinformation, foreign agents, media discourse, manipulative technologies.

Введение. Информационное противостояние между Российской Федерацией и западными странами, в особенности Соединенными Штатами Америки, стало определяющим фактором международных отношений в последнее десятилетие. Американские средства массовой информации превратились в сложный инструмент ведения информационной войны против России, оказывая значительное влияние на общественное сознание, политические процессы и международное восприятие страны в целом. В период с 2014 по 2025 год методы и стратегии информационного воздействия претерпели существенную эволюцию –от относительно простых форм пропаганды до сложных когнитивных технологий.

Как отмечает российский политолог, кандидат физико-математических наук, доктор политических наук, профессор МГУ имени М.В.Ломоносова, А.В.Манойло,

«информационное противоборство стало неотъемлемым компонентом современных международных отношений, определяющим их характер и динамику» [2].

Понятие информационной войны. Понятийный аппарат в сфере информационного противоборства продолжает формироваться, демонстрируя значительное разнообразие терминов. В российском понимании информационная война определяется как «противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем» (Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 5 декабря 2016 г. № 646) [1].

Русский ученый, публицист, философ, один из первых теоретиков информационной войны, С. П. Расторгуев, дает более расширенное определение: «Информационная война – это открытые и скрытые целенаправленные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере» [5].

А.В. Манойло характеризует информационную войну как «вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия» [2]. Информационные операции же представляют собой разведывательные, оперативные комбинации на каналах открытых телекоммуникационных

сетей (ОТКС) в основе которых лежит симбиоз трех групп методов: оперативной контурной работы, оперативно-технические и оперативно-разыскные. Они представляют собой последовательность информационных вбросов, разделенных периодами тишины, т.е. экспозиции.

В западной традиции понятие «информационная война» более тесно связано с военными действиями и направлено преимущественно на военное и разведывательное сообщества противника. Американский теоретик, исследователь в области национальной безопасности и кибервойн, Мартин К. Либицки выделяет семь видов информационных войн в рамках вооруженного конфликта: командно-управленческая война, разведывательная война, электронная война, психологическая война, хакерская война, экономическая война и кибервойна [9].

Ближе к современному пониманию информационного противоборства стоит термин «когнитивная война», под которым понимаются действия государства или влиятельных групп для манипулирования механизмами познания противника и его населения, чтобы ослабить, влиять на него или даже подчинить себе. Этот термин начал активно использоваться в Соединенных Штатах с 2017 года, но был выведен в публичное пространство лишь в 2020 году аналитиками НАТО [9]. Когнитивная война сочетает новейшие кибертехнологии и человеческую составляющую «мягкой силы», а также манипулятивные аспекты психологических операций (PSYOPS), находясь на пересечении двух операционных областей, которые ранее управлялись по отдельности: психологические операции и операции влияния, с одной стороны, и кибероперации – с другой.

Исторический контекст. Исторические корни информационной войны США против России восходят к периоду Холодной войны. 18 августа 1948 года Совет национальной безопасности США принял директиву 20/1 «Цели США в войне против России», которая считается началом информационной войны США против СССР [15]. Эта директива объявила войну качественно нового типа, где оружием служит информация, а борьба ведется за целенаправленное изменение общественного сознания.

Качественно новым этапом стало принятие в январе 1981 года серии секретных докладов по национальной безопасности (NSDD), в которых руководство подрывной деятельностью против СССР официально перешло от спецслужб к вашингтонским чиновникам высшего государственного уровня. В директиве NSDD-75 предписывалось прямое вмешательство во внутренние дела соцстран с целью подрыва их режимов, ставка делалась на создание и консолидацию «внутренних оппозиционных сил», которые при поддержке извне должны были добиться захвата власти и политической переориентации своих стран на Запад [16].

Современный этап информационного противоборства активизировался после 2014 года на фоне событий вокруг Крыма и вооруженного конфликта в Донбассе (2014-2022 гг.). Российские СМИ отмечают, что с этого периода начинается систематическая работа американских медиа по формированию негативного образа России как агрессора и нарушителя международного права [4]. В опубликованной в июле 2023 года «Стратегии по операциям в информационной среде на 2023 год» Пентагона прямо говорится о необходимости создания специальных «информационных сил», чтобы «получать и поддерживать информационные преимущества... для успешной работы в информационном пространстве» [14].

Методы и инструменты. Американские СМИ проводят систематическую работу по формированию в мировом общественном мнении негативного восприятия России и ее политики. В одном из главных инструментов пропаганды Америки является американская международная общественная радиокомпания, Voice of America, где осуществляется продвижение нарративов о «российской агрессии», «нарушении прав человека» и «угрозе демократическим ценностям». Эти нарративы затем тиражируются медиа других стран, создавая единое информационное поле противодействия российским интересам. С начала проведения специальной военной операции было опубликовано огромное количество статей со следующими заголовками: *«Burn the Ukrainian Children? Genocidal Rant is Now Mainstream Russian Propaganda», «Russia Unleashes 'Missile Terror' on Ukrainian Civilians, Falsely Claims Military Targets», «Putin's Fraudulent Foundation for Attacking Ukraine», «Russia Creates Ukraine Disaster, Then Claims Credit For 'Humanitarian' Aid», «Lavrov echoes debunked Kremlin narratives to justify war, undermine NATO».*

Посмотрим на них с точки зрения лингвистики. Они являются яркими примерами использования языка как инструмента информационного воздействия и формирования общественного мнения в условиях конфликта. Общая стратегия всех заголовков –полярное противопоставление «добра и зла»: с одной стороны –агрессивный, лживый и аморальный образ России, с другой – невинные жертвы (Украина, гражданское население). Это классический прием создания «карикатурного образа врага».

«Burn the Ukrainian Children?» (Сжечь украинских детей?): «Burn» (Сжечь) – глагол с экстремально высокой эмоциональной нагрузкой. Он ассоциируется с варварством, жестокостью и абсолютным злом. Сам вопрос в форме риторического утверждения звучит как обвинение [6].

«Genocidal Rant» (Геноцидальная тирада): *«Genocidal»* – самое тяжелое юридическое и моральное обвинение, которое только можно выдвинуть. Его использование сразу переводит дискуссию в плоскость преступления против человечности. *«Rant»* –не «речь» или «заявление», а именно «тирада», «исступленная речь». Это слово автоматически дискредитирует говорящего, представляя его иррациональным и одержимым [6].

«Unleashes 'Missile Terror'» (Развязала «ракетный террор»): *«Terror» (Террор)* – ключевое слово. Это не просто «атака» или «обстрел», а «террор», что прямо отсылает к тактике террористов, цель которых –запугивание мирного населения [13].

«Putin's Fraudulent Foundation» (Мошенническое обоснование Путина): *«Fraudulent» (Мошеннический, обманный)* – это не «спорный» или «ошибочный», а именно «мошеннический», то есть основанный на сознательном обмане [12].

«Debunked Kremlin narratives» (Опровергнутые нарративы Кремля) –словосочетание «кремлевские нарративы» само по себе стало в западной прессе штампом, обозначающим официальную, но ложную версию событий. Эпитет *«debunked» (опровергнутые)* усиливает эффект, указывая на то, что эти утверждения уже были разоблачены [8].

К сожалению, список подобных пропагандистских заголовков можно продолжать бесконечно. Конечно, клевета, дезинформация, информационная истерия, драматизация, прослеживаемая в содержании медиакампании, создает мощь пропагандисткой машины Америки. Однако можно с уверенностью утверждать, что использование таких продуманных до мелочей стилистических приемов, даже риторических уничтожений, в политическом дискурсе, демонстрирует некую игру в демократию со стороны США.

Представленные заголовки – это не нейтральная отчетность, а мощный инструмент информационной кампании. Через тщательный подбор лексики, синтаксических конструкций и прямого приписывания мотивов они формируют у аудитории строго определенное, эмоционально окрашенное восприятие конфликта. Их цель – не информировать, а убеждать и мобилизовывать, создавая однозначный и непримиримый образ врага.

СМИ активно обвиняют российские войска в масштабных военных преступлениях и нарушении демократии, международного права, распространяют фейковую информацию о запрете свободы слова на территории РФ, о совершении насилия, пыток, намеренных убийств украинских детей российскими войсками на территории Украины, не предоставляя конкретных доказательств и обоснований, игнорируя и ставя вне поле зрения те жесточайшие события, происходящие на Донбассе с весны 2014 года. Безусловно, это делает их домыслы и тиражируемые фантазии спекулятивными и вводящими в заблуждение.

Кроме этого, активно ведется продвижение прозападных политических ориентаций, противопоставленных традиционным российским ценностям, сепаратистских настроений, провоцирующих вовлечение граждан в незаконные публичные акции, ложной информации, направленной на зловещую деморализацию РФ.

Еще одним важным аспектом является идеологическая поддержка санкционной политики и международной изоляции России. Через медиаканалы формируется представление о

необходимости и оправданности ограничительных мер против российских официальных лиц, предприятий и отраслей экономики. Создается образ России как страны-изгоя, что соответствует интересам американской внешней политики.

С точки зрения безопасности, американские медиа участвуют в сборе информации о внутрироссийских процессах. Как отмечается в Доктрине информационной безопасности РФ 2016 года, одной из потенциальных угроз безопасности России является «наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях», а также усиление деятельности организаций, «осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса». [1]

Заключение. Проведя исследования, можно сделать вывод, что воздействие американских СМИ как инструмента информационной войны масштабно и значимо. Американские медиа – это инструмент противодействия России, целью которого является формирование негативного образа страны на международной арене и поддержка санкционного режима. На основе анализа контента «Voice of America» выявляются ключевые тематические линии и риторические приемы, направленные на формирование негативного образа России, дискредитацию ее внутренней и внешней политики, а также поддержку санкционного режима и международной изоляции страны. Особое внимание уделяется механизмам распространения дезинформации, использованию эмоционально окрашенных ярлыков и манипулятивных техник в медиаинформационном пространстве. В этих условиях укрепление информационного суверенитета России и развитие эффективной системы противодействия иностранному информационному влиянию становятся задачами стратегической важности.

Список источников и литературы

1. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента Российской Федерации от 5 дек. 2016 г. № 646. Доступ из справ.-правовой системы «Гарант».
2. Манойло А.В. Информационные войны и психологические операции. М.: Лаборатория знаний, 2021. 180 с.
3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2030 года: утв. Указом Президента Российской Федерации от 12 апр. 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Пешкова Н.В., Филимонова Е.Ю., Умарова С.И. и др. Использование тактики обвинения в формировании негативного имиджа России в зарубежном политическом дискурсе (на материале американских СМИ) // Наука и школа. — 2016. — № 4. — С. 228–232. — URL: https://cyberleninka.ru/article/n/ispolzovanie-taktiki-obvineniya-v-formirovanii-negativnogo-imidzha-rossii-v-zarubezhnom-politicheskom-diskurse-na-materiale/viewer.
5. Расторгуев С.П. Информационная война. М.: Радио и связь, 1999. 416 с.
6. Burn the Ukrainian Children? Genocidal Rant is Now Mainstream Russian Propaganda // Voice of America. — 2022. — 27 октября. URL: https://www.voanews.com/a/burn-the-ukrainian-children-genocidal-rant-is-now-mainstream-russian-propaganda/6808030.html (медиакомпания признана иноагентом на территории Российской Федерации).
7. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // Lawfare Research Paper Series. 2023. No. 12. P. 34-56.
8. Lavrov echoes debunked Kremlin narratives to justify war, undermine NATO // Voice of America. — 2025. — 21 января. URL: https://www.voanews.com/a/lavrov-echoes-debunked-kremlin-narratives-to-justify-war-undermine-nato/7945306.html (медиакомпания признана иноагентом на территории Российской Федерации).
9. Libicki M. What is Information Warfare? Washington: National Defense University, 1995. 89 p.
10. McCombs M., Shaw D. The Agenda-Setting Function of Mass Media // Public Opinion Quarterly. 1972. Vol. 36. No. 2. P. 176-187.
11. Noelle-Neumann E. The Spiral of Silence: Public Opinion – Our Social Skin. 2nd ed. Chicago: University of Chicago Press, 1993. 244 p.
12. Putin’s Fraudulent Foundation for Attacking Ukraine // Voice of America. — 2022. — 10 марта. URL: https://www.voanews.com/a/fact-check-putin-s-fraudulent-foundations-for-attacking-ukraine/6743310.html (медиакомпания признана иноагентом на территории Российской Федерации).
13. Russia Unleashes ‘Missile Terror’ on Ukrainian Civilians, Falsely Claims Military Targets // Voice of America. — 2022. — 13 октября. URL: https://www.voanews.com/a/6788372.html (медиакомпания признана иноагентом на территории Российской Федерации).
14. United States. Department of Defense. 2023 Cyber Strategy of the Department of Defense: [Стратегия кибербезопасности Министерства обороны на 2023 год]. Washington, D.C. : DOD, 2023. 36 p. — URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY.PDF — Загл. с экрана. — Текст: электронный.

15. United States. National Security Council. NSC 20/1 : U.S. Objectives with Respect to Russia: [цели США в отношении России] : [top secret report]. 1948, Aug. 18. 23 p. // Foreign Relations of the United States (FRUS). 1948. Vol. I (part 2). P. 624–628. — URL: https://history.state.gov/historicaldocuments/frus1948v01p2/d21.

16. United States. President (1981-1989: Reagan). National Security Decision Directive Number 75: U.S. Relations with the USSR: [директива в области национальной безопасности № 75: Отношения США с СССР]. 1983, Jan. 17. 7 p. – URL: https://www.reaganlibrary.gov/archives/solution/nsdd75-us-relations-ussr – Текст: электронный.

Цао Юнь,
аспирант кафедры социальной философии,
факультет гуманитарных и социальных наук,
Российский университет дружбы народов (РУДН),
E-mail: 1042248312@pfur.ru

Cao Yun,
PhD student, Department of Social Philosophy,
Faculty of Humanities and Social Sciences,
Peoples' Friendship University of Russia (RUDN University),
E-mail: 1042248312@pfur.ru

МЕДИА И КОММУНИКАЦИЯ В ЦИФРОВУЮ ЭПОХУ: СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

MEDIA AND COMMUNICATION IN THE DIGITAL AGE: SOCIO-PHILOSOPHICAL ANALYSIS OF INFORMATION SECURITY

Аннотация. В статье рассматриваются трансформации медиа и коммуникационных практик в условиях цифровизации общества через призму социальной философии. Особое внимание уделяется вопросам информационной безопасности в контексте изменения природы публичного пространства, формирования цифровой идентичности и трансформации социальных связей. Автор анализирует философские основания современных медиакоммуникаций и их влияние на структуру общественных отношений.

Ключевые слова: цифровые медиа, коммуникация, информационная безопасность, социальная философия, публичное пространство, цифровая идентичность

Abstract. The article examines the transformations of media and communication practices under the conditions of the digitalization of society through the lens of social philosophy. Particular attention is paid to issues of information security in the context of the changing nature of the public sphere, the formation of digital identity, and the transformation of social ties. The author analyses the philosophical foundations of contemporary media communications and their impact on the structure of social relations.

Key words: digital media, communication, information security, social philosophy, public sphere, digital identity.

Цифровая революция последних десятилетий радикально трансформировала не только технологический ландшафт, но и фундаментальные основы социальной коммуникации. Современное общество характеризуется беспрецедентной интенсивностью информационных потоков, новыми формами медиации социальных отношений и качественно иными механизмами производства и распространения знания. В этом контексте вопросы информационной

безопасности выходят за рамки технических проблем и приобретают глубокое социально-философское измерение.

Как отмечает М. Кастельс, мы живем в «сетевом обществе», где информация становится ключевым ресурсом власти, а коммуникационные технологии определяют структуру социальных взаимодействий [4, с. 34]. Эта трансформация требует переосмысления классических философских категорий публичности, приватности, идентичности и социальной связи в контексте цифровой реальности.

1. Трансформация публичного пространства в цифровую эпоху

Цифровые медиа радикально изменили природу публичного пространства, которое в классической социальной философии рассматривалось как сфера рационального дискурса и формирования общественного мнения. Ю. Хабермас описывал публичную сферу как пространство критической рефлексии, где граждане, освобожденные от партикулярных интересов, участвуют в рациональной дискуссии [11, с. 89].

Однако цифровизация создает принципиально новую модель публичности. Социальные медиа формируют то, что можно назвать «сетевой публичностью», характеризующейся одновременной массовостью и фрагментацией. С одной стороны, цифровые платформы обеспечивают беспрецедентный доступ к публичному дискурсу, демократизируя производство и распространение информации. С другой стороны, алгоритмическая кураторство создает «пузыри фильтров», где пользователи взаимодействуют преимущественно с единомышленниками [7, с. 156].

Эта трансформация имеет прямые последствия для информационной безопасности. Фрагментация публичного пространства создает условия для манипуляции общественным сознанием, распространения дезинформации и поляризации общества. Феномен «эхо-камер» в социальных сетях препятствует критическому осмыслению информации и способствует радикализации взглядов.

2. Цифровая идентичность и проблема аутентичности

Цифровая эпоха порождает новые формы конструирования идентичности, что становится важнейшим аспектом информационной безопасности. В отличие от традиционного понимания идентичности как относительно стабильного самоопределения личности, цифровая идентичность характеризуется множественностью, перформативностью и постоянной реконфигурацией.

Социальные сети создают условия для того, что Э. Гоффман называл «представлением себя другим» в повседневной жизни, но в радикально усиленной форме [2, с. 67]. Пользователи конструируют множественные цифровые персоны, адаптируя самопрезентацию к различным

платформам и аудиториям. Это порождает философскую проблему аутентичности: насколько цифровые репрезентации соответствуют «подлинному» Я?

С точки зрения информационной безопасности, эта проблема имеет несколько измерений. Во-первых, множественность и изменчивость цифровой идентичности создает уязвимости для идентификационного мошенничества и кражи личных данных. Во-вторых, коммерциализация персональных данных превращает идентичность в товар, что ставит под вопрос автономию личности [3, с. 178]. В-третьих, использование технологий глубокой фальсификации (deepfake) размывает границы между реальным и симулированным, создавая кризис доверия.

3. Медиатизация социальных отношений и проблема социальной связи

Цифровые медиа не просто опосредуют социальные отношения, но трансформируют саму природу социальной связи. Если в классической социологии (Э. Дюркгейм, Ф. Тённис) социальная солидарность основывалась на разделяемых ценностях, коллективных представлениях или непосредственном взаимодействии, то в цифровую эпоху социальные связи все чаще опосредуются технологическими платформами и алгоритмами.

Это создает парадоксальную ситуацию: с одной стороны, цифровые технологии обеспечивают возможность поддержания связей с большим количеством людей на любом расстоянии; с другой стороны, исследования показывают рост социальной изоляции и ослабление «сильных связей». Ш. Тёркл описывает это как состояние «одиночества вместе», когда физическое присутствие не гарантирует подлинной коммуникации [8, с. 234].

С позиций информационной безопасности, важно понимать, что медиатизация социальных отношений создает новые формы уязвимости. Зависимость от цифровых платформ для поддержания социальных связей делает пользователей восприимчивыми к манипуляциям со стороны корпораций и государств. Сбор данных о социальных взаимодействиях позволяет создавать детальные профили пользователей, которые могут использоваться для таргетированного влияния [9, с. 267].

4. Информационная безопасность как социально-философская проблема

Традиционно информационная безопасность рассматривалась преимущественно в технических терминах: защита данных, криптография, кибербезопасность. Однако социально-философский анализ показывает, что это лишь один аспект более фундаментальной проблемы.

Информационная безопасность в широком смысле связана с защитой базовых условий возможности рациональной коммуникации и формирования достоверного знания. Когда информационная среда загрязнена дезинформацией, манипуляциями и пропагандой, под угрозой оказывается не только безопасность данных, но и эпистемологические основания общества.

З. Бауман описывает современность как состояние «текучей современности», характеризующейся неопределенностью и постоянными изменениями [1, с. 112]. В условиях информационного изобилия и дефицита внимания граждане сталкиваются с трудностями в различении достоверной информации и дезинформации. Это создает кризис доверия к институтам и экспертному знанию.

Более того, коммерциализация информационного пространства и доминирование алгоритмических систем рекомендаций создают то, что можно назвать «эпистемологическим неравенством». Крупные технологические корпорации обладают беспрецедентным доступом к информации о пользователях и возможностью формировать их информационную среду, в то время как сами пользователи имеют ограниченное понимание принципов работы этих систем [6, с. 345].

5. К философии цифровой безопасности: нормативные принципы

Социально-философский анализ медиа и коммуникации в цифровую эпоху позволяет сформулировать некоторые нормативные принципы, которые должны лежать в основе политики информационной безопасности.

Во-первых, принцип информационной автономии: граждане должны иметь реальную возможность контролировать свои персональные данные и понимать, как они используются. Это требует не только правового регулирования, но и развития цифровой грамотности [10, с. 189].

Во-вторых, принцип транспарентности алгоритмов: системы, которые формируют информационную среду и влияют на принятие решений, должны быть прозрачными и подотчетными. Это особенно важно для алгоритмов, используемых в социальных сетях, поисковых системах и системах искусственного интеллекта.

В-третьих, принцип защиты публичной сферы: информационная безопасность должна включать меры по защите публичного дискурса от манипуляций, обеспечению разнообразия источников информации и противодействию дезинформации без ущерба для свободы слова.

В-четвертых, принцип цифровой солидарности: в эпоху глобальных информационных потоков необходимо развивать механизмы международного сотрудничества в области информационной безопасности, основанные на разделяемых ценностях и взаимном уважении [5, с. 278].

Заключение. Социально-философский анализ медиа и коммуникации в цифровую эпоху раскрывает, что информационная безопасность представляет собой не только техническую, но и фундаментальную социальную проблему. Цифровизация трансформирует природу публичного пространства, идентичности и социальных связей, создавая новые формы уязвимости и требуя переосмысления традиционных подходов к безопасности.

Обеспечение информационной безопасности в широком смысле предполагает защиту эпистемологических и коммуникативных условий функционирования демократического общества. Это требует интегрированного подхода, сочетающего технические решения, правовое регулирование, развитие цифровой грамотности и формирование этических норм использования цифровых технологий.

Дальнейшие исследования в этой области должны развивать междисциплинарный диалог между философией, социологией, правом и компьютерными науками для выработки комплексных стратегий обеспечения информационной безопасности в цифровую эпоху.

Список источников и литературы:

1. Бауман З. Текучая современность. СПб.: Питер, 2008. 240 с.
2. Гоффман И. Представление себя другим в повседневной жизни. М.: КАНОН-пресс-Ц, 2000. 304 с.
3. Зубофф Ш. Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти. М.: Издательство Института Гайдара, 2022. 784 с.
4. Кастельс М. Информационная эпоха: экономика, общество и культура. М.: ГУ ВШЭ, 2000. 608 с.
5. Най Дж. Будущее власти. М.: АСТ, 2014. 444 с.
6. О’Нил К. Математика разрушения. Как большие данные увеличивают неравенство и угрожают демократии. М.: АСТ, 2018. 416 с.
7. Парайзер И. За стеной фильтров. Что Интернет скрывает от вас. М.: Альпина Бизнес Букс, 2012. 304 с.
8. Тёркл Ш. Одиночество вместе. М.: АСТ, 2014. 480 с.
9. Флориди Л. Четвертая революция. Как инфосфера меняет лицо человеческой реальности. М.: Дело, 2020. 352 с.
10. Флореди Л. Этика информации. М.: Праксис, 2017. 368 с.
11. Хабермас Ю. Структурное изменение публичной сферы: исследования относительно категории буржуазного общества. М.: Весь Мир, 2016. 344 с.

Рима Андраниковна Карапетян,
студентка магистратуры,
Дипломатическая академия МИД России,
E-mail: rimm.karapetyan@gmail.com

Rima A. Karapetyan,
master's student,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: rimm.karapetyan@gmail.com

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА ОРГАНИЗАЦИЮ И ПРЕДОСТАВЛЕНИЕ КОНСУЛЬСКИХ УСЛУГ

THE IMPACT OF DIGITALIZATION ON THE ORGANIZATION AND PROVISION OF CONSULAR SERVICES

Аннотация. Автором исследуется комплексное влияние процессов цифровизации на функционирование консульских служб в современном мире. Анализируя примеры из различных стран и международных организаций, автор рассматривает трансформацию традиционных консульских процессов через внедрение цифровых технологий. В статье рассматриваются преимущества цифровизации для эффективности консульских услуг и удовлетворения потребностей граждан, а также выявляются критические вызовы. Исследование показывает, что цифровая трансформация не является самоцелью, а скорее средством для повышения качества обслуживания граждан и укрепления национальной безопасности в эпоху быстрых технологических изменений.

Ключевые слова: цифровизация, консульские услуги, электронные визы, искусственный интеллект, трансформация дипломатии, электронное правительство.

Abstract. The author examines the complex impact of digitalisation processes on the functioning of consular services in the modern world. Analysing examples from various countries and international organisations, the author considers the transformation of traditional consular processes through the introduction of digital technologies. The article discusses the advantages of digitalisation for the efficiency of consular services and meeting the needs of citizens, and identifies critical challenges. The study shows that digital transformation is not an end in itself, but rather a means to improve the quality of service to citizens and strengthen national security in an era of rapid technological change.

Key words: digitalisation, consular services, electronic visas, artificial intelligence, transformation of diplomacy, digital government.

Развитие информационных технологий в начале двадцать первого века революционизировало практически все аспекты деятельности государственных учреждений, не

исключая консульских служб, которые исторически полагались на бюрократические процессы, основанные на бумажной документации и непосредственном взаимодействии между должностными лицами и гражданами [2;9]. Консульские учреждения, традиционно рассматриваемые как воплощение государственного суверенитета и представительства за границей, сталкиваются с необходимостью адаптации к современным требованиям цифровой эпохи, характеризующейся беспрецедентным объемом информационного обмена, растущими ожиданиями граждан к скорости и удобству предоставления услуг, а также постоянно усложняющимися угрозами кибербезопасности [6;8]. Согласно исследованиям специалистов в области цифровой трансформации государственных структур, процесс перевода консульских функций в цифровую среду представляет собой не просто техническое обновление, а глубокую переоценку того, как государства взаимодействуют со своими гражданами за рубежом и как они управляют проверкой подлинности личности в контексте растущей глобальной мобильности [2;7].

Масштабы трансформации, которую переживают консульские службы, становятся очевидными при рассмотрении конкретных инициатив, предпринимаемых различными странами. Вместе с тем процесс цифровизации консульских служб не является гладким и прямолинейным. Международные исследования выявляют значительные различия между странами в уровне готовности к цифровой трансформации, во многом определяемые наличием необходимой инфраструктуры, уровнем развития информационных технологий и принятием соответствующего законодательства [7]. Более того, цифровизация консульских служб порождает новые вызовы.

Концептуальные основы цифровой трансформации дипломатии. Цифровая трансформация дипломатии представляет собой явление, которое ученые определяют как интеграцию цифровых технологий в традиционные дипломатические практики с целью перестройки способов, которыми нации взаимодействуют, ведут переговоры и взаимодействуют на глобальной сцене [2]. Феномен этой трансформации не ограничивается просто заменой почтовой корреспонденции электронной почтой или использованием видеоконференций вместо личных встреч; это фундаментальное переосмысление роли информационных потоков, скорости коммуникации и природы самого дипломатического процесса [2]. Исследователи отмечают, что традиционная дипломатия, которая исторически полагалась на формальные дипломатические каналы, физические посольства и представительства, а также медленные процессы консультаций, постепенно трансформируется в смешанную форму, известную как «гибридная дипломатия», которая объединяет элементы традиционных методов с современными цифровыми платформами и инструментами [7].

Академические работы по этой тематике выделяют несколько ключевых измерений цифровой трансформации дипломатии [6]. Первое измерение касается убеждений и ценностей дипломатических учреждений относительно роли информационных технологий в их функционировании. Когда-то цифровые инструменты рассматривались как вспомогательные средства для коммуникации, но теперь они воспринимаются как интегральная часть дипломатической стратегии и инструмент достижения внешнеполитических целей [6]. Второе измерение охватывает процедурные изменения, то есть трансформацию реальных методов и процессов, которые используют дипломаты в своей работе. Это включает внедрение новых протоколов коммуникации, создание специальных цифровых отделов в министерствах иностранных дел, разработку стратегий управления кризисами с использованием социальных медиа и внедрение систем анализа больших данных для мониторинга глобальных тенденций [6]. Третье измерение связано с институциональными изменениями, касающимися трансформации самих дипломатических организаций, их структуры, функций и отношений с другими государственными и негосударственными акторами.

Развитие цифровой политики в области международных отношений. В последние пять лет наблюдается значительное ускорение в разработке государственных стратегий в области цифровой политики, непосредственно влияющих на консульские услуги [3]. Несколько развитых стран приняли комплексные стратегии цифровой внешней политики, которые определяют приоритеты государства в области цифровизации международных отношений. Ряд исследователей относит такие страны, как Австралию, Данию, Францию, Нидерланды и Швейцарию, к пионерам в этом отношении, поскольку они разработали документы стратегического характера, которые определяют цели и методы применения цифровых технологий в дипломатической деятельности [3]. Данные стратегии обычно охватывают несколько ключевых областей: цифровую инфраструктуру, роль цифровизации в развитии, кибербезопасность, экономическую конкурентоспособность и защиту прав человека в цифровой сфере [3].

Важной особенностью развития цифровой политики является признание того, что цифровая трансформация не может быть уделом только министерств иностранных дел. Напротив, это требует координации между различными государственными органами, включая министерства технологии, финансов, обороны, а также привлечения частного сектора и гражданского общества [3]. Такой подход, известный как «whole-of-government» и «whole-of-society», предполагает, что успешная цифровая трансформация дипломатических и консульских служб может быть достигнута только при условии скоординированного взаимодействия множественных акторов, каждый из которых вносит свой уникальный вклад в процесс трансформации. Примером такого

подхода является создание в Австралии специальной Международной группы по работе с кибер- и критическими технологиями, которая объединяет представителей пяти различных министерств, офиса премьер-министра, генерального прокурора и других государственных учреждений [3].

Технологические инновации в консульских услугах. Одной из наиболее видимых и практически значимых форм цифровизации консульских услуг является внедрение систем электронных виз (e-visa) и цифровых авторизаций [5;9]. Традиционная система выдачи виз, при которой физическое паспортное буклет отправляется в консульство для вклеивания виз и последующего возврата заявителю, постепенно дополняется или заменяется системами электронных виз, при которых разрешение на въезд хранится в электронной форме и может быть проверено пограничными органами через компьютеризованные системы контроля [8]. Государственный департамент США разрабатывает технологию Digital Visa Authorization (DVA), которая позволит выдавать разрешения на въезд в цифровой форме вместо традиционных виз, размещаемых в паспортах [9]. Данная технология опирается на интеграцию с системой валидации документов Таможенной службы США (U.S. Customs and Border Protection Document Validation program), которая оповещает авиакомпании об наличии у путешественника действительной визовой авторизации [9].

Примеры успешной реализации систем электронных виз можно найти в различных регионах мира. Япония запустила систему JAPAN eVISA, позволяющую граждан определенных стран (включая Австралию, Бразилию, Канаду, Соединенное Королевство и США) подавать заявления на туристические визы онлайн и получать электронное разрешение на въезд без необходимости посещения консульства [5]. Вьетнам реализовал политику выдачи электронных виз всем иностранным гражданам, начиная с августа 2023 года, что значительно упростило процесс получения разрешения на въезд для туристов и деловых путешественников [8]. Европейский Союз разработал систему ETIAS (European Travel Information and Authorization System), которая планировалась к внедрению в 2024 году и будет отслеживать граждан стран, не требующих виз для краткосрочного пребывания в странах Шенгенского пространства [8].

Преимущества электронных систем виз очевидны. Прежде всего, они значительно сокращают время, необходимое для получения визы, позволяя заявителям подавать документы и получать решение через интернет без необходимости физического визита в консульство. Во-вторых, системы e-visa снижают затраты на обработку заявлений, так как они автоматизируют многие рутинные процессы проверки документов и верификации информации. В-третьих, электронные системы обеспечивают лучший контроль над пограничной безопасностью, так как информация о всех выданных визах централизованно хранится и легко доступна пограничным

органам. Наконец, такие системы повышают удобство для пользователей, особенно для граждан, проживающих далеко от консульств, или лиц с ограниченной физической мобильностью.

Искусственный интеллект и системы автоматизации роботизированных процессов (RPA) постепенно внедряются в процессы обработки документов в консульских службах, обеспечивая беспрецедентный уровень эффективности и точности [4]. Технологии машинного обучения позволяют системам автоматически сканировать, классифицировать и анализировать большие объемы вспомогательных документов, которые приложены к визовым и паспортным заявлениям, в доли времени, которое требовалось бы человеческому оператору [4]. Системы на основе искусственного интеллекта способны выявлять аномалии, такие как несоответствия в документах, отсутствующую информацию или потенциально поддельные документы, и затем направлять внимание консульских работников на эти проблемные случаи [4]. Такой подход позволяет консульским офицерам сосредоточиться на более сложных случаях, требующих человеческого суждения и дипломатической чувствительности, особенно в критических ситуациях, когда речь может идти о жизни и смерти граждан, находящихся в опасности.

Внедрение ИИ-систем в консульских операциях предполагает использование многоязычной поддержки, что позволяет системам обрабатывать документы на различных языках и адаптироваться к особенностям различных правовых систем и культурных контекстов [4]. Эти системы могут быть обучены распознавать специфические элементы документов, такие как печати, подписи и защитные элементы, характерные для подлинных государственных документов различных стран. Кроме того, ИИ-системы способны выявлять закономерности в мошеннических действиях, используя исторические данные о поддельных документах и мошеннических попытках, что позволяет предупредить новые формы мошенничества еще до того, как они получат широкое распространение.

Однако внедрение систем искусственного интеллекта в консульские операции сопровождается серьезными вызовами. Одной из основных проблем является обеспечение справедливости и отсутствия предвзятости в алгоритмах машинного обучения, так как эти алгоритмы «обучаются» на исторических данных, которые могут содержать структурные предубеждения. Кроме того, необходимо обеспечить прозрачность в работе этих систем, чтобы граждане и должностные лица понимали, на основе каких критериев принимаются решения о выдаче или отказе в выдаче виз. Требуется также разработка механизмов обжалования решений, принятых автоматизированными системами, чтобы граждане имели возможность опротестовать неправильные решения и добиться справедливого результата.

Заключение. Цифровизация консульских услуг представляет собой одно из наиболее значительных изменений в функционировании государственных учреждений в современную

эпоху, несущее с собой как огромные возможности, так и серьезные вызовы. Исследование показывает, что страны по всему миру осознают необходимость трансформации традиционных, основанных на бумажной документации процессов в направлении цифровых, автоматизированных систем, которые могут обрабатывать растущий объем заявлений более эффективно, обеспечивать лучшее обслуживание граждан и повышать национальную безопасность. Примеры из практики различных государств подтверждают, что технологические инновации, включая электронные визы, искусственный интеллект, биометрические системы и облачные хранилища данных, оказывают измеримое положительное влияние на эффективность и качество консульских операций.

Однако успешная цифровизация консульских услуг не является автоматическим следствием просто внедрения новых технологий. Как показывает опыт различных стран, реализация цифровых систем требует комплексного подхода, включающего надлежащее финансирование, подготовку персонала, разработку адекватного законодательства, обеспечение защиты данных и выявление возможных негативных последствий для уязвимых групп населения. Особое внимание должно быть уделено обеспечению справедливого доступа к цифровым услугам для всех граждан, независимо от их возраста, уровня цифровой грамотности, места проживания или экономического статуса. Кроме того, при использовании систем искусственного интеллекта в консульских операциях необходимо внедрить строгие меры контроля для предотвращения встроенных предубеждений и дискриминации.

Список источников и литературы:

1. Center for Technology in Government. Internationalizing Digital Government Research. University at Albany. // [Электронный ресурс] URL: https://www.ctg.albany.edu/publications/intl_dg_research/ (дата обращения: 25.12.2025).

2. Digital Transformation in Diplomacy. Sustainability Directory. Term Definition. // [Электронный ресурс] URL: https://pollution.sustainability-directory.com/term/digital-transformation-in-diplomacy/ (дата обращения: 25.12.2025).

3. Diplo Foundation. Global Trends in Digital Foreign Policy and Diplomacy Strategies. [Электронный ресурс] URL: https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/global-trends-in-digital-foreign-policy-and-diplomacy-strategies/ (дата обращения: 25.12.2025).

4. Diplomatic Academy. How Artificial Intelligence Can Modernize Consular Services. // [Электронный ресурс] URL: https://diplomaticacademy.us/2025/05/18/artificial-intelligence-consular-services/ (дата обращения: 25.12.2025).

5. Ministry of Foreign Affairs, Japan. The JAPAN eVISA System (Electronic Visa). [Электронный ресурс] URL: https://www.mofa.go.jp/j_info/visit/visa/visaonline.html (дата обращения: 25.12.2025).

6. Oxford University. The Digitalization of Diplomacy: Working Paper. // [Электронный ресурс] URL: https://www.qeh.ox.ac.uk/sites/default/files/2023-08/DigDiploROxWP2.pdf (дата обращения: 25.12.2025).

7. Rise of Hybrid Diplomacy: From Digital Adaptation to Digital Adoption. [Электронный ресурс] URL: Oxford University Press. International Affairs, Vol. 98, No. 2. https://academic.oup.com/ia/article/98/2/471/6540781 (дата обращения: 25.12.2025).

8. Talent Everywhere. How Digital Innovations Are Transforming Immigration Systems Worldwide. // [Электронный ресурс] URL: https://www.talenteverywhere.org/Mobility-News/Article/how-digital-innovations-are-transforming-immigration-systems-worldwide (дата обращения: 25.12.2025).

9. U.S. State Department. Digital Visa Authorization (DVA) Proof of Concept. Travel.State.Gov. // [Электронный ресурс] URL: https://travel.state.gov/content/travel/en/News/visas-news/digital-visa-authorization-dva-proof-of-concept.html (дата обращения: 25.12.2025).

Секция А3

«Право и безопасность в цифровой среде: ИКТ, искусственный интеллект и нейротехнологии»

Ольга Игоревна Агнистикова,
к.филол.н, ассистент кафедры национальных и глобальных медиа,
Казанский (Приволжский) федеральный университет,
E-mail: agniolya570@yandex.ru

Olga I. Agnistikova,
Ph.D, assistant, Department of National and Global Media,
Kazan (Volga region) Federal University,
E-mail: agniolya570@yandex.ru

РЕГУЛИРОВАНИЕ ИКТ: ПРОТИВОДЕЙСТВИЕ «ЦИФРОВОМУ КОЛОНИАЛИЗМУ»

ICT REGULATION: COUNTERING DIGITAL COLONIALISM

Аннотация. Тяготение технологической индустрии к паттернам доминирования усилило риторику «цифрового колониализма» как угрозы для стран Глобального Юга. Один из ответов на новые вызовы лежит в плоскости регулирования. Принятие специфических норм в идеале может смягчить неравенство распределения власти и предотвратить «хищнические» практики со стороны транснациональных корпораций. Оптика деколонизации позволяет по-новому взглянуть на правила, нацеленные на сектор ИКТ.

Ключевые слова: регулирование информационно-коммуникационных технологий, пользовательские данные, цифровой колониализм, технологическая деколонизация.

Abstract. The tech industry's gravitation toward patterns of dominance have intensified the rhetoric of digital colonialism as a threat to countries in the Global South. One answer to these new challenges lies in regulation. Adopting specific norms could ideally mitigate power imbalances and prevent predatory practices by transnational corporations. A decolonization lens allows for a fresh look at regulations targeting the ICT sector.

Key words: regulation of information and communications technology, user data, digital colonialism, technological decolonization.

Динамика власти в цифровую эпоху: уязвимое положение Глобального Юга. Технологические инновации, концентрируя в себе масштабный потенциал для трансформаций во многих сферах общественной жизни, воспроизводят господствующую структуру властных отношений. Такова позиция, получившая широкое признание на мировом уровне и нашедшая отражение в таких концепциях, как «цифровой капитализм», «цифровой неолиберализм», «платформенный капитализм», «надзорный капитализм» («капитализм слежения»), «цифровой колониализм». Среди этих терминов особенно выделяется последний, поскольку он подчеркивает по умолчанию менее сильное и влиятельное положение одной группы стран (Глобальный Юг) перед другой (Глобальный Север). В связи с этим вопрос установления регулирующих рамок для такой бурно развивающейся сферы, как технологическая, встает наиболее остро. Причина тому кроется в гегемонистском статусе транснациональных корпораций, ставших главными игроками в этой сфере, устанавливающих тренды и определяющих «правила игры». Эти корпорации, обладая колоссальными ресурсами, разработали большие языковые модели и приняли установку по экспансии своих продуктов и услуг во все регионы мира. Стоит признать, что здесь наблюдается тесное пересечение таких устремлений с геополитическими амбициями отдельных государственных акторов. Такое положение не может не вызывать беспокойство, поскольку ставит под угрозу хрупкий баланс сил на международной арене и международное согласие. Страны Глобального Юга могут оказаться при этом «разменной монетой» или «пешками» в руках могущественных игроков. Недопустимость этой ситуации усугубляется асимметрией между существенным вкладом Глобального Юга в развитие технологической индустрии и мизерными преимуществами, которые получают эти регионы. Эта асимметрия концептуализируется как «цифровой колониализм».Колониальные паттерны были выявлены во многих процессах, связанных с информационно-коммуникационным сектором: разработка («невидимый труд», эксплуатация данных), внедрение (передача технологий без учета местного контекста), управление, регулирование [1]. Например, страны Африки, Латинской Америки и Центральной Азии нередко не участвуют в обсуждениях глобальных принципов ИИ в необходимом объеме или не оказывают значимого влияния на принятие соответствующих политических решений [2]. Напротив, Глобальный Север продолжает получать несправедливо большую выгоду (экономическую, технологическую, политическую, социально-культурную), экспансивно захватывая новые рынки и наращивая свое господство. В этих условиях в разных уголках мира растет сопротивление, которое концептуализируется как «цифровая деколонизация». Существуя и развиваясь нередко на «этаже» гражданского общества, оно переходит и на «этаж» государственной политики. Рассмотренную динамику важно учитывать, поскольку она дает возможность оценить, направлено ли регулирование в том или ином государстве на противодействие «цифровому колониализму» или нет.

Цифровой суверенитет. В качестве аналитической рамка оценки противодействия цифровому колониализму целесообразно использовать концепт «цифровой суверенитет». Он вбирает способность субъекта контролировать собственную цифровую инфраструктуру, регулировать потоки данных в пределах своей юрисдикции и управлять платформами в

соответствии со своими законами, ценностями и национальными интересами. Метафорически говоря, это способность субъекта в полной мере контролировать свою цифровую судьбу.

Так, с перспективы укрепления цифрового суверенитета принимаемые государством акты можно анализировать по нескольким аспектам:

1) Инфраструктурный – владение и контроль над подводными кабелями, центрами обработки данных, сервисами облачных вычислений и другими объектами цифрового мира;

2) Регулятивно-управленческий – участие в формировании норм, регулирующих деятельность технологических компаний и других игроков индустрии ИИ;

3) Суверенитет данных – способность к юридическому и техническому контролю над данными;

4) Культурно-эпистемический – защита местных языков, поддержание культурного разнообразия.

Ряд актов, принятых странами Глобального Юга, действительно в определенной мере отражает эту логику цифрового суверенитета. Так, Стратегия цифровой трансформации для Африки на 2020–2030 годы опирается на идеи развития инфраструктуры [3]. В русле таких установок действует и Акт о защите персональной информации [4], который отражает растущую важность проблематики защиты пользовательских данных. Индия тоже находится на передовой, активно продвигая суверенитет через введение обязанности хранения данных своих граждан на серверах внутри страны. По тому же пути локализации данных пошел и Вьетнам, а Индонезия ввела правила, требующие от иностранных цифровых платформ открытия местных офисов.

Заключение. Проанализированные акты часто фрагментарны, в этой связи требуется более последовательная политика. Для этого, как представляется, Глобальный Юг должен скоординировать свои усилия по деколонизации сферы ИКТ.

Список источников и литературы:

1. Decolonising AI: What, Why and How? [Электронный ресурс]. URL: https://rai.ac.uk/decolonising-ai-what-why-and-how/ (дата обращения: 10.11.2025).

2. G20 Summit: Why India refused to sign Osaka declaration on global data flow [Электронный ресурс]. URL: https://www.timesnownews.com/india/article/g20-summit-why-india-refused-to-sign-osaka-declaration-on-global-data-flow/446887 (дата обращения: 10.11.2025).

3. The African Union's Digital Transformation Strategy for Africa (2020–2030). URL: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf. (дата обращения: 10.11.2025).

4. Protection of Personal Information Act. URL: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (дата обращения: 10.11.2025).

Алла Юрьевна Ястребова,
доктор юридических наук, доцент,
профессор кафедры международного права
Дипломатическая академия МИД России
E-mail: kafedra.mp@dipacademy.ru;

Игорь Олегович Анисимов,
кандидат юридических наук,
декан международно-правового факультета
Дипломатическая академия МИД России
E-mail: kafedra.mp@dipacademy.ru

Alla Yu.Yastrebova,
Doctor of Law, Professor of the Department of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
E-mail: kafedra.mp@dipacademy.ru;

Igor O. Anisimov,
Ph.D. in Law, Dean of the Faculty of International Law,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia
E-mail: kafedra.mp@dipacademy.ru

МЕЖДУНАРОДНО-ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

INTERNATIONAL LEGAL PROTECTION OF PERSONAL DATA IN THE MODERN INFORMATION SPACE

Аннотация. Авторами проанализировано содержание основных международно-правовых актов универсального и регионального уровня, направленных на защиту персональных данных. Изучено действующее в указанной сфере законодательство Российской Федерации, определены правовые приоритеты защиты персональных данных в информационном пространстве. В связи с тем, что персональные данные принадлежат к области частной жизни и определяются семейными, социальными, культурными особенностями, индивидуально присущими каждому лицу, обоснована значимость научных позиций по осуществлению их защиты.

Ключевые слова: персональные данные, права человека, трансграничная передача данных, цифровые технологии, предупреждение деяний, относящихся к киберпреступности.

Abstract. The authors analyzed the main international legal instruments on universal and regional level aimed at protecting personal data. The national legislation of the Russian Federation in the above field is studied, and the legal priorities of personal data protection in information space are examined. Since personal data pertain to private life and are determined by family, social and cultural

peculiarities, inherent in every human being, the importance of scientific positions on exercise such protection is substantiated.

Keywords: personal data, human rights, cross-border data transfer, digital technologies, prevention of cybercrimes.

Защита персональных данных людей тесно связана с обеспечением права на частную жизнь и безопасности индивидуальных цифровых идентификаторов личности в информационной среде. Существующие международно-правовые стандарты прав человека и продвижение искусственного интеллекта требуют переосмысления в сфере совместного применения. Сегодня прогресс цифровых средств очевиден; его использование в общении, доступе к социальным услугам, транспортном и банковском обслуживании, трудоустройстве, дистанционной торговле, логистике и образовании, электронном документообороте означает удовлетворение базовых потребностей человека в этом пространстве.

Конвенция ООН против киберпреступности, которая принята резолюцией Генеральной Ассамблеи 79/243 от 24 декабря 2024 г. [7], содержит правовые основы межгосударственного контроля над воздействием новейших цифровых технологий и предупреждения угроз, которые могут нести информационно-коммуникационные системы (ИКС). К запретным деяниям отнесены незаконный доступ и перехват передачи электронных данных, неправомерное использование электронных устройств, подлог, хищение и мошенничество с использованием ИКС, сексуальные преступления в отношении несовершеннолетних лиц, распространение интимных изображений без согласия лиц, на них представленных, отмывание преступных доходов (ст. 7-17). Борьба с подобной деятельностью включает необходимость усиленной защиты личных сведений и учитывает социальную уязвимость детей. При передаче персональных данных государства-участники должны обеспечить, чтобы на полученные данные распространялись эффективные и надлежащие гарантии, предусмотренные национальной нормативно-правовой базой (ч. 2 ст. 36). Персональные данные (ПД), согласно Конвенции, понимаются как любая информация, относящаяся к определенному или определяемому физическому лицу (п. g) ст. 2).

Наиболее детально международно-правовые аспекты современного права на защиту персональных данных регламентированы на региональном уровне [6, с.245].

Соглашение СНГ о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными 2020 г. [9]. также включает расширенную дефиницию ПД и причисляет к ним любую информацию, прямо или косвенно относящуюся к физическому лицу, которое идентифицировано или может быть идентифицировано (ст. 1). Соглашением

гарантирована защита ПД от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения или иных запретных действий; обозначается принцип конфиденциальности получения и содержания запросов участников и целевого использования личной информации (ч. 1, 2 и 5 ст. 10).

Соглашение об информационном взаимодействии государств-участников СНГ в области цифрового развития общества 2020 г. [10]. закрепляет основные направления сотрудничества, в том числе, развитие регионального цифрового пространства и информационной безопасности и обеспечение доступа к информационно-коммуникационным технологиям в соответствии с национальным законодательством сторон (ст. 3).

Федеральный закон Российской Федерации «О персональных данных» № 152-ФЗ от 27 июля 2006 г. [11]. устанавливает, что физическое лицо как субъект ПД может быть прямо и косвенно определенным или определяемым (ч. 1 ст. 3). В его содержании учтены биометрические персональные данные, представляющие собой сведения, идентифицирующие физиологические и биологические особенности личности и использующиеся оператором для ее установления (ч. 1 ст. 11). Порядок трансграничной передачи ПД предполагает обеспечение их конфиденциальности и безопасности при обработке (ч. 2 ст. 12).

Российскими учеными-правоведами высказано мнение о том, что правоприменитель считает значимым выделить точные критерии, которые позволяют однозначно определить само содержание персональных данных людей [1, с. 51]. Они также считают, что укрепление приоритета защиты прав гражданина в качестве базового принципа отношений в сфере сбора, обработки и использования ПД становится особенно актуальным в связи с созданием цифрового профиля личности [5].

Конвенция СНГ о правах и основных свободах человека 1995 г. [8]. формулирует право человека на уважение его личной и семейной жизни, неприкосновенность жилища и тайну переписки (ч. 1 ст. 9). Персональные данные принадлежат к частной жизни и определяются семейными, социальными, культурными особенностями, индивидуально присущими каждому лицу. Право на защиту ПД выражено в универсальных договорах, регламентирующих правовой статус детей. Представляется, что при цифровизации социальной сферы должны быть гарантированы, прежде всего, права и потребности людей в сфере приватности и личной безопасности. В.А.Карташкин справедливо указывает, что под влиянием информационной среды и предполагаемых ею фундаментальных изменений для каждого человека и общества в целом стабильной международно-правовой основой защиты продолжает оставаться Билль о правах, который выступает общим источником понимания и традиционных, и цифровых прав человека, находящихся в органическом единстве между собой [3, с. 949].

Принятие новых международно-правовых актов СНГ в сфере защиты персональных данных направлено не только на унификацию и гармонизацию законодательства государств-участников, но и на совершенствование существующего национального законодательства. Изменения, внесенные в Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных» с 1 сентября 2022 г. (установлена обязанность операторов уведомлять Роскомнадзору о начале или осуществлении любой обработки персональных данных, за исключением случаев, когда данные обрабатываются в целях защиты безопасности государства и общественного порядка; сокращены сроки предоставления информации Роскомнадзору; определены обязанности оператора в случае компрометации персональных данных; скорректирован порядок обработки данных по требованию физлица, а также предусмотрен новый порядок трансграничной передачи персональных данных) отражают общую тенденцию усиления контроля за любыми операциями, проводимыми операторами с ПД субъекта. Особое внимание как на региональном, так и на национально-правовом уровне уделяется контролю за трансграничной передачей ПД.

Учредительные договоры Европейского союза учитывают право человека на защиту персональных данных (ч. 1 ст. 16 Договора о функционировании ЕС (ДФЕС), в редакции Лиссабонского договора 2007 г.) [12]. Установление правил по защите ПД данных физических лиц и свободе их перемещения возложено на Европейский парламент, Европейский совет и государства – члены ЕС (ч. 2 ст. 16 ДФЕС). Хартия об основных правах ЕС помимо прямо закрепляет право на защиту ПД и требует от государств-членов добропорядочных и целевых условий их обработки, с согласия заинтересованного лица или по иным правомерным основаниям, установленным законом (ч. 2 ст. 8) [13]. В ней содержится право каждого лица на доступ к собранным данным и устранение в них ошибок, под контролем независимых органов (ч. 3 ст.8).

В свою очередь, П.А. Калиниченко и М.В. Некотенева также указывают на необходимость защиты ПД при осуществлении исследований генома человека и отмечают, что с целью обеспечения безопасности геномной информации «ряд актов вторичного права ЕС <…> регулирует отношения, связанные с защитой прав личности при сборе, хранении и обработке персональных данных» [2, с. 75].

Регламент Европейского парламента и Совета ЕС № 679/2016 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/45/ЕС (Общий Регламент о защите персональных данных) определяет ПД как любую информацию, относящуюся к физическому лицу, с помощью которой такое лицо может быть идентифицировано прямо или косвенно, в частности,

посредством таких критериев, как имя, идентификационный номер, сведения о местоположении, идентификатор в режиме онлайн, или через один или несколько признаков, связанных с физической, психологической, генетической, умственной, экономической, культурной или социальной идентичностью указанного физического лица (ч. 1 ст. 4) [14]. Российские ученые-правоведы отмечают, что эффективность защиты персональных данных требует не только гармонизации принципов такой защиты, но и «средств их применения в столь быстро меняющейся и высоко технологической области» и условий трансграничной передачи указанных данных [4, с. 122].

В содержании Регламента Европейского парламента и Совета ЕС №2018/1725 от 23 октября 2018 г. о защите физических лиц при обработке персональных данных, осуществляемой государственными учреждениями, органами, службами и агентствами Союза, и о свободном обращении таких данных, а также об отмене Регламента (ЕС) 45/2001 и Решения 1247/2002/ЕС [15] приведен более широкий перечень правовых определений. В частности, в ст. 3 вводятся термины «оперативные персональные данные» (персональные данные, обработанные государственными органами стран – членов ЕС) и «пользователь» (физическое лицо, оперирующее в пределах распределенной сети или оборудования, подконтрольного органам государства – члена ЕС). Ст. 52 Регламента №2018/1725 учреждает Европейский надзорный орган по защите данных (European Data Protection Supervisor). Раздел 3 гл. 4 Регламента №2018/1725 предусматривает обязательство органов государств – членов ЕС обеспечивать безопасность своих электронных сетей; защиту информации, переданной, полученной и обработанной с помощью терминального оборудования, относящегося к сайтам и мобильным приложениям; запрет на использование информации о пользователях в маркетинговых целях. Регламент включает нормы, обеспечивающие создание технических условий для поддержания безопасности персональных данных и их обработки.

Систематизация защиты персональных данных становится особой правовой потребностью в связи с тем, что постоянно расширяется сфера их использования в деятельности государств и юридических лиц. Правовые определения ПД тесно связаны с понятием информации, прямо или косвенно идентифицирующей личность. По нашему мнению, каждое обозначенное направление эволюции информационных технологий должно быть согласовано с общими стандартами защиты права человека на частную жизнь и правом лица на идентификацию.

Список источников и литературы:

1. Добробаба М.Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О.Е.Кутафина (МГЮА). 2023. № 2. С. 42-52.

2. Калиниченко П.А., Некотенева М.В. Особенности правового регулирования геномных исследований на международном и европейском уровне // Вестник университета имени О.Е. Кутафина (МГЮА). — 2020. — №4. — С. 68-78. https://doi.org/10.17803/2311-5998.2020.68.4.068-078

3. Карташкин В.А. Цифровые права человека: международно-правовое и социальное измерения // Вестник РУДН, серия «Социология». 2022. № 4. С. 949-962.

4. Полякова Т.А., Химченко А.И. Актуальные организационно-правовые вопросы трансграничной передачи персональных данных // Право: журнал Высшей школы экономики. — 2013. — № 1. — С. 113-122.

5. Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // Lex Russica. 2020. Т. 73. № 2. С. 33-43.

6. Ястребова А.Ю., Анисимов И.О. Осуществление права человека на защиту персональных данных: отдельные международно-правовые аспекты, опыт России и СНГ // Вестник ученых-международников. 2022. № 3 (21). С. 241-266.

7. Конвенция ООН против киберпреступности. Принята резолюцией Генеральной Ассамблеи 79/243 от 24 декабря 2024 г. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 18.10.2025).

8. Конвенция СНГ о правах и основных свободах человека 1995 г., действует в редакции Протокола от 14 октября 2022 г. URL: https://www.consultant.ru/document/cons_doc_LAW_6966/ (дата обращения: 18.10.2025).

9. Соглашение СНГ о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными 2020 г. // URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/59889/ (дата обращения: 18.10.2025).

10. Соглашение об информационном взаимодействии государств-участников СНГ в области цифрового развития общества 2020 г. // URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/59889/ (дата обращения: 18.10.2025).

11. Федеральный закон о персональных данных от 27 июля 2005 г. № 152-ФЗ. СЗ РФ от 31 июля 2005 г. № 31 (ч. I). Ст. 3451. Действует в редакции от 7 июля 2025 г.

12. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community(2007/C306/01). [Электронный ресурс]. – URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A12007L%2FTXT (дата обращения: 18.10.2025).

13. Charter of fundamental rights of European Union (2000/C364/01). [Электронный ресурс]. – URL:https://www.europarl.europa.eu/charter/pdf/text_en.pdf (дата обращения: 18.10.2025).

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Электронный ресурс]. – URL:https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R0679&qid=1626789259064 (дата обращения: 18.10.2025).

15. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) [Электронный ресурс]. – URL: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN (дата обращения: 18.10.2025).

Елена Михайловна Маслова,
магистр по направлению «Международное частное право»
ФГБОУ ВО «Санкт-Петербургский государственный университет»,
специалист по предоставлению помощи населению
Международного комитета Красного Креста,
E-mail: elena.maslova97@mail.ru

Дмитрий Николаевич Васьков,
директор департамента международных связей
Министерства международных и внешнеэкономических связей
Свердловской области, старший преподаватель кафедры
зарубежного регионоведения
ФГАОУ ВО «Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина»,
E-mail: vaskov.dm@yandex.ru

Elena M. Maslova,
Master of International Private Law,
St. Petersburg State University,
Specialist in Population Assistance,
International Committee of the Red Cross,
E-mail: elena.maslova97@mail.ru

Dmitry N. Vaskov,
Director of the International Relations Department,
Ministry of International and Foreign Economic Relations
of Sverdlovsk Oblast, Senior Lecturer,
Department of Foreign Regional Studies,
Ural Federal University
named after the first President of Russia B. N. Yeltsin,
E-mail: vaskov.dm@yandex.ru

ИНСТИТУТ ЭЛЕКТРОННОЙ ЛЕГАЛИЗАЦИИ ДОКУМЕНТОВ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

THE INSTITUTE OF ELECTRONIC DOCUMENT LEGALIZATION: CHALLENGES AND PROSPECTS FOR IMPLEMENTATION IN THE RUSSIAN FEDERATION

Аннотация. В работе предлагается комплексный анализ института электронный легализации документов в контексте имплементации механизма электронного апостиля в Российской Федерации. Исследуются проблемы необходимости приведения национального законодательства в соответствии с новыми технологическими реалиями, анализируется зарубежный опыт внедрения системы e-App. В работе выявлены правовые коллизии, связанные с определением статуса электронных официальных документов и применением цифрового формата легализации.

Ключевые слова: электронная легализация, апостиль, e-App, цифровизация, официальные документы, консульская легализация, электронный реестр апостилей, нотариальное заверение.

Abstract. The authors conduct a comprehensive analysis of the framework for electronic document legalization, focusing on the implementation of the e-apostille mechanism in the Russian Federation. The study investigates the imperative to adapt national legislation to new technological realities and critically assess international experience with the e-App system. The research identifies specific legal collisions arising from defining the status of electronic public documents and employing digital formats for legalization.

Key words: electronic legalization, apostille, e-App, digitalization, public documents, consular legalization, e-Register, notarization.

Легализация различных видов документов. Интенсификация международного взаимодействия обусловливает необходимость быстрой передачи данных и оперативного документооборота на международном уровне. Документ, предназначенный для использования за рубежом, подлежит легализации. Однако существуют случаи, когда процедура легализации может не применяться:

Во-первых, это возможно в тех случаях, когда между государствами заключен договор о правовой помощи.

Во-вторых, не могут быть использованы по назначению, а следовательно, и легализованы документы и акты, противоречащие национальному законодательству страны, а также наносящие вред интересам государства предъявления документа.

За исключением указанных случаев отмены легализации, законодательство большинства стран мира для установления подлинности и законности документов требует их нотариально заверенного перевода и легализации, осуществляемой в форме консульской легализации или проставления апостиля (в соответствии с Гаагской конвенцией 1961 г.). Необходимо отметить, что механизм легализации применяется только к официальным документам. Конвенция устанавливает широкое понятие «официального документа», что приводит к различной правоприменительной практике, поскольку его окончательная классификация отнесена к национальному праву государства-участника. Так, положения Гаагской конвенции не уточняют, следует ли проставлять апостиль только на подлинные официальные документы или апостиль может также проставляться на заверенные копии официальных документов. Возникает коллизионная ситуация, при которой копия административного документа, имеющего прямое отношение к коммерческой и таможенной операции, в одном государстве рассматривается в

качестве одной из категорий официального документа (нотариальный акт), а в другом государстве — как документ, который не подлежащий легализации.

Кроме того, существуют государства, применяющие Гаагскую конвенцию к документам, имеющим прямое отношение к коммерческой и таможенной операциям, не требуют обязательного удостоверения в виде консульской легализации или проставления апостиля. Подобную практику подтверждает Специальная комиссия в пункте 15 Заключений и рекомендаций от 2012 г. [1]. Связно это, в первую очередь, с тем, что национальное законодательство этих государств определяет документы, связанные с осуществлением внешнеэкономической и таможенной деятельности, как «официальные документы», подлежащие апостилированию. Так, в Испании свидетельство о государственной регистрации продукции подлежит апостилированию, использование на территории Новой Зеландии сертификата происхождения товара, экспортной лицензии и коммерческих счет-фактур требует также проставление специального штампа апостиль.

Таким образом, несмотря на введение механизма упрощённого удостоверения подлинности документа, все же возникает необходимость выяснения требований, предъявляемых к определенным категориям документов, в конкретном государстве.

Формирование и реализация программы электронного апостилирования. Научно-технический прогресс, не предвиденный при принятии Гаагской конвенции 1961 года, обусловил необходимость адаптации механизма апостилирования к современным реалиям. В ответ на вызовы цифровизации в 2006 году была разработана программа e-App, предусматривающая внедрение электронного апостиля (e-Apostille) и электронного реестра (e-Register). Несмотря на преимущества системы – ускорение процедуры, снижение рисков подделки и повышение надежности верификации – её имплементация породила правовые коллизии.

К настоящему времени из 122 государств, являющихся Договаривающими сторонами Гаагской конвенции, 48 стран внедрили один или оба компонента e-App [3]. Текущая статистика свидетельствует, что несмотря на преимущества системы электронного апостилирования, не все страны одинаково воспринимают процесс внедрения новых технологий для работы с документами.

Многие государства широко трактуют текст Гаагской конвенции для реализации ее основной цели. Однако стоит отметить, что Гаагская конвенция не содержит статей, прямо указывающих на возможность использования новейших технологий в процессе легализации документов. Исходя из этого, некоторые страны по-прежнему используют бумажный апостиль и ведут в бумажном виде реестр зарегистрированных апостилей. В результате, в рамках Гаагской конвенции сложилась практика двух вариантов легализации иностранных официальных

документов: проставление физического апостиля и апостилирование с использованием новых компьютерных технологий. В свою очередь, подобные режимы способствуют возникновению следующих юридических коллизий, которые, на наш взгляд, свидетельствуют о прямом нарушении обязательств по Гаагской конвенции:

Во-первых, государство-участник Гаагской конвенции, полностью завершивший процесс внедрения программы электронного апостилирования и использующий только электронный апостиль для легализации официального документа, отказывается принимать бумажный апостиль на своей территории.

Во-вторых, некоторые страны-участницы Гаагской конвенции, где апостиль проставляется в бумажном виде, отказываются принимать электронный апостиль. После прекращения проставления апостилей на аллонже с 2013 г. [2]. Республика Молдова столкнулась с отказом принятия её электронного апостиля со стороны Итальянской Республики и Российской Федерации.

Таким образом, разработанная в 2006 г. программа электронного апостилирования адаптирует действие Гаагской конвенции к реалиям XXI века и современным компьютерным технологиям. С одной стороны, широкая терминология, используемая в Гаагской конвенции, позволяет без изменения текста международного договора преобразовывать институт апостилирования официальных документов посредством ведения электронных реестров и проставления апостиля в электронном формате. С другой стороны, отсутствие в тексте данного международного договора статей, прямо указывающих на безоговорочную необходимость государств признавать или использовать электронный апостиль, приводит к разнообразной практике среди стран-участниц, а также формированию нескольких режимов в рамках Гаагской конвенции: полный переход на проставление и принятие апостилей в электронном формате, применение и признание апостилей исключительно бумажного формата, смешанный порядок оформления апостиля.

Проблемы внедрения института электронной легализации в России. Утвержденное Постановлением Правительства Российской Федерации от 20.03.2021 г. № 436 Положение об особенностях обращения с запросом о проставлении апостиля, проставления апостиля и направления запросов, предусмотренных статьей 9 Федерального закона «О проставлении апостиля на российских официальных документах, подлежащих вывозу за пределы территории Российской Федерации», в электронном виде и(или) с использованием информационно-телекоммуникационных сетей, ведения реестра апостилей в электронном виде, обеспечения дистанционного доступа к сведениям о проставленных апостилях [4] должно способствовать

процессу апостилирования официальных документов в более доступном, надежном, безопасном и удобном формате.

Вместе с тем, использование нововведения требует определенных дополнительных ресурсов, а рассмотрение рекомендаций Специальной комиссии по оптимизации процесса легализации официальных документов накладывает определенные трудности.

Анализ региональной практики (на примере Москвы и Свердловской области) демонстрирует различные подходы к использованию e-App. В Москве реализована частично электронная процедура, требующая последующего предоставления оригиналов документов. В Свердловской области сохраняется необходимость личного посещения ведомств, что нивелирует преимущества дистанционного формата.

Заключение. Ключевыми препятствиями для эффективного функционирования института электронного апостиля в РФ являются:

1. отсутствие законодательно закрепленной обязанности органов предоставлять образцы подписей и печатей в электронные базы данных;
2. сохранение бумажного формата официальных документов;
3. отсутствие единой системы верификации скан-копий.

Разрешение указанных проблем требует комплексной модернизации системы документооборота и создания национальной цифровой инфраструктуры.

Список источников и литературы:

1. Conclusions and Recommendations of the Special Commission on the practical operation of the Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions (2 to 12 February 2009) [Электронный ресурс] // Hague Conference on Private International Law. URL: https://assets.hcch.net/docs/5bf65314-4f55-42b5-9b0c-770f2bfccd37.pdf (дата обращения: 10.11.2025).
2. Cu privire la modificarea şi completarea unor hotărîri ale Guvernului: Guvernul Hotărâre din 18.09.2013 № 739 // Monitorul Oficial al Republicii Moldova. 2013. № 212. Art. 848.
3. Implementation Chart of the e-APP [Электронный ресурс] // Hague Conference on Private International Law. URL: https://assets.hcch.net/docs/b697a1f1-13be-47a0-ab7e-96fcb750ed29.pdf (дата обращения: 10.11.2025).
4. Об утверждении Положения об особенностях обращения с запросом о проставлении апостиля, проставления апостиля и направления запросов, предусмотренных статьей 9 Федерального закона «О проставлении апостиля на российских официальных документах, подлежащих вывозу за пределы территории Российской Федерации», в электронном виде и(или) с использованием информационно-телекоммуникационных сетей, ведения реестра апостилей в электронном виде, обеспечения дистанционного доступа к сведениям о проставленных апостилях: Постановление Правительства Российской Федерации от 20.03.2021 № 436 [Электронный ресурс] // Государственная система правовой информации: официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202103230025?pageSize=10&index=1 (дата обращения: 10.11.2025).

Полина Андреевна Ветрова,
Студент I курса,
факультет юриспруденции,
Московский государственный юридический университет
имени О. Е. Кутафина,
E-mail: vvetrovavetrovaa@gmail.com

Polina A. Vetrova,
1st year student,
faculty of law, Moscow state law University
name O. E. Kutafina,
E-mail: vvetrovavetrovaa@gmail.com

СООТНОШЕНИЕ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ И ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

BALANCE BETWEEN THE RIGHT TO PRIVACY AND ACCESS TO PERSONAL DATA IN ORDER TO ENSURE PUBLIC SAFETY

Аннотация. В исследовании изучено соотношение ценности обеспечения общественной безопасности и права на неприкосновенность частной жизни при обработке сведений, прямо или косвенно определяющих человека, которые созданы посредством использования информационных технологий коммуникации. Автор выдвигает гипотезу о нарушении в современном обществе баланса между двумя вышеуказанными ценностями со смещением приоритетов на общественные интересы и расширением прав уполномоченных органов по доступу к персональной информации пользователей технологий. Выдвигаемая гипотеза раскрывается через анализ источников права государств разных правопорядков, регулирующих вопрос доступа органов государственной власти к информации о субъектах персональных данных.

Ключевые слова: персональные данные, публичный порядок, неприкосновенность частной жизни, ИКТ.

Abstract. The author examines balance between the value of ensuring public safety and the right to privacy when processing information that directly or indirectly defines a person, which is created through the use of information communication technologies. The author hypothesizes that there is a violation in modern society of the balance between the two above-mentioned values, with a shift in priorities to public interests and an expansion of the rights of authorized bodies to access the personal information of technology users. The hypothesis put forward is revealed through an analysis of the sources of law of states of different legal systems governing the issue of access of public authorities to information about personal data subjects.

Key words: personal data, public order, privacy, ICT.

В современном мире цифровизации жизненных процессов информация, сгенерированная человеком при использовании технических средств связи, создает массивный объем данных, обработка которых представляет интерес для различных категорий лиц: от государственных до коммерческих.

С одной стороны, доступ к такой информации позволяет принимать наиболее точные решения с высокой скоростью, так как для сведений, созданных при использовании информационно-телекоммуникационных технологий (далее – ИКТ), характерна постоянная обновляемость и актуальность. С другой стороны, обработка третьими лицами сгенерированной во время интернет-сессии и других технологий связи информации создает условия тотальной слежки за субъектом, которого такая информация определяет.

Из вышеуказанных обстоятельств проистекает дилемма: какой из двух ценностей отдать предпочтение при регулировании случаев обработки информации о пользователе ИКТ? Праву на защиту от вмешательства в частную жизнь субъекта или гарантии обеспечения общественной безопасности и публичного порядка? Поднимаемая автором проблема присуща правопорядкам стран разных регионов мира: в настоящем исследовании будет изучено регулирование вопроса баланса ценностей в правовом поле Российской Федерации, Европейского Союза (далее – ЕС) и Соединённых Штатов Америки (далее – США).

Определение права на неприкосновенность частной жизни. В статье 8 Европейской конвенции о защите прав человека и основных свобод 1950 г. (далее – ЕКПЧ) принцип невмешательства в частную жизнь определяется через право на уважение частной и семейной жизни, жилища и корреспонденции; не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья, нравственности или защиты прав и свобод других лиц [4].

В статье 23 Конституции Российской Федерации указывается, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. А также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения [1].

Кроме решения суда основанием для ограничения прав и свобод, в том числе права на неприкосновенность частной жизни, является необходимость обеспечения безопасности граждан и защита конституционного строя [1].

Соотношения права на неприкосновенность частной жизни и ценности общественной безопасности. В развитие вопроса соотношения права на защиту от произвольного вмешательства в личную жизнь и необходимостью сохранить общественный порядок в Европейском Союзе была принята Директива (ЕС) 2016/680, которая определила основу для обработки персональных данных государственными органами. Согласно статье 8 Директивы (ЕС) 2016/680, обработка оправдана только тогда, когда она служит чрезмерным интересом общественности к предотвращению преступности и обеспечению общественной безопасности, и она всегда должна проводиться с соблюдением принципов необходимости, пропорциональности и ограниченности цели [5]. Это гарантирует, что инструменты, используемые для защиты общественной безопасности, не подрывают основные права и свободы, которые они предназначены для защиты.

Иллюстрирующим аксиому, заложенную в законодательстве ЕС, примером является решение Суда Европейского Союза C-623/17 в 2020 г., в рамках которого организации, выступающие за неприкосновенность частной жизни и цифровые права (La Quadrature du Net, French Data Network и др.), а также профессиональные сообщества (Ordredes barreaux francophones et germanophones) утверждали, что даже под предлогом обеспечения национальной безопасности тотальная слежка за всем населением является несоразмерным и незаконным нарушением основных прав. Правительства Франции и Бельгии оппонировали, что постоянная угроза терроризма и тяжких преступлений представляет собой серьезную угрозу национальной безопасности, которая оправдывает исключительные меры, в том числе массовый сбор данных. Суд ЕС постановил: национальные законы государств-членов ЕС, предусматривающие общее и неизбирательное хранение данных о трафике и местоположении, как правило, противоречат законодательству ЕС. Такие меры представляют собой особенно серьезное нарушение прав на неприкосновенность частной жизни и защиту данных (статьи 7 и 8 ЕКПЧ). Однако в этом же решении Суд ЕС впервые признал, что экзистенциальная угроза потенциально может служить оправданием для таких крайних мер [6].

Другим прецедентом современности стала новость о выдаче Управлением расследований Министерства внутренней безопасности США ордера, обязывающего разработчика ИИ-систем OpenAI передать данные пользователя ChatGPT в рамках расследований. Ордер был выдан судом штата Мэн и связан с делом о расследовании сети сайтов на даркнете. Следствие запросило у OpenAI данные, которые способствуют установлению личность пользователя: историю

диалогов, IP-адреса, контактную информацию и данные платежей. Согласно судебным документам, компания предоставила по запросу таблицу Excel с запрошенной информацией [7].

Применительно к Российской Федерации детальное изучение вопроса допустимости вмешательства в личную жизнь человека представлено в определениях и постановлениях Конституционного Суда, который выработал правовые позиции, касающиеся допустимого ограничения прав и свобод человека и гражданина, в частности: ограничения конституционных прав должны быть необходимыми и соразмерными конституционно признаваемым целям таких ограничений; ограничения не могут посягать на самое существо того или иного права и приводить к утрате его реального содержания; при допустимости ограничения того или иного права в соответствии с конституционно одобряемыми целями государство, обеспечивая баланс конституционно защищаемых ценностей и интересов, должно использовать не чрезмерные, а только необходимые и строго обусловленные этими целями меры [2].

Тенденция на смещение приоритета в сторону защиты и сохранения публичного порядка обществ и общественной безопасности в ущерб гарантии на невмешательство в частную жизнь человека прослеживается в опубликованном 01 ноября 2025 года постановлении Правительства Российской Федерации от 30.10.2025 № 1698 «О внесении изменения в постановление Правительства Российской Федерации от 23 сентября 2020 г. № 1526», которое внесло изменения в правила хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, продлив срок хранения и, следовательно, обеспечения доступа уполномоченных государственных органов к информации, сгенерированной посредством [3].

Заключение. Из вышеуказанного можно сделать вывод об усилении тенденции на смешение приоритетов в сторону обеспечения нерушимости публичного порядка в ущерб неприкосновенности частной жизни и запрета на вмешательство в нее со стороны органов государственной власти. Порядок реализации личных заградительных права, которые заключаются в обязанности государства не только самому не пересекать границы, установленные такими правами, но и обеспечить условия непреодоления этих границ другими субъектами права, претерпевает изменения. Рассмотренные выше судебные решения и подзаконные акты демонстрируют тезис о новой расстановке приоритетов в вопросе баланса общественной

безопасности и невмешательства в частную жизнь не в пользу последнего. Причинами происходящих событий можно считать исторические обстоятельства неопределенности ущерба, который может быть нанесен вследствие реализации новых угроз национальной безопасности, исходящих от нестандартных видов нарушений и нарушителей.

Список источников и литературы:

1. Конституция Российской Федерации от 12.12.1993 [Электронный ресурс] // Pravo.gov.ru. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102027595 (дата обращения: 25.10.2025).

2. Постановление Конституционного Суда РФ от 14 ноября 2005 г. № 10-П [Электронный ресурс] / Pravo.gov.ru. URL: http://pravo.gov.ru/proxy/ips/?docrefs.xml=&oid=102083973 (дата обращения: 27.10.2025).

3. Постановление Правительства Российской Федерации от 30.10.2025 № 1698 «О внесении изменения в постановление Правительства Российской Федерации от 23 сентября 2020 г. № 1526» [Электронный ресурс] // Publication.pravo.gov.ru. URL:http://publication.pravo.gov.ru/document/0001202511010038?utm_source=Securitylab.ru&index=1 (дата обращения: 25.10.2025).

4. Convention for the Protection of Human Rights and Fundamental Freedoms [e-source] / European Court of Human Rights // URL: https://www.echr.coe.int/european-convention-on-human-rights (дата обращения: 01.11.2025).

5.Directive (EU) 2016/680 of the European Parliament and of the Councilon the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [e-source] / EUR-lex // URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng (дата обращения: 03.10.2025).

6. Judgment of the Court (Grand Chamber) of 6 October 2020. Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [e-source] /Info.Curia // URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7108220 (дата обращения: 01.10.2025).

7. Thomas Brewster. DHS Ordered OpenAI To Share User Data In First Known Warrant For ChatGPT Prompts // Forbes / URL: https://www.forbes.com/sites/thomasbrewster/2025/10/20/openai-ordered-to-unmask-writer-of-prompts/ (дата обращения: 01.11.2025).

Гайсин Реналь Радикович,
аспирант кафедры международного и европейского права
Казанского (Приволжского) федерального университета,
E-mail: G-Renal@mail.ru

Renal R. Gaisin,
Postgraduate Student of the Department of International and European Law,
Kazan (Volga region) Federal University (Kazan),
E-mail: G-Renal@mail.ru

МЕЖДУНАРОДНОЕ РЕГУЛИРОВАНИЕ КИБЕРНЕЙРОБЕЗОПАСНОСТИ

INTERNATIONAL REGULATION OF CYBERNEUROSECURITY

Аннотация. Работа посвящена исследованию проблем кибернейробезопасности, возникающих в связи с интеграцией нейронауки и информациионно-коммуникационных технологий (ИКТ). В исследовании раскрыты основные международные акты и организации, занимающиеся вопросами кибернейробезопасности. Автором предлагаются конкретные направления совершенствования международного правового регулирования кибернейробезопасности.

Ключевые слова: кибернейробезопасность, искусственный интеллект, киберугрозы, нейротехнологии.

Abstract. This paper examines cyberneurosecurity issues arising from the integration of neuroscience and information and communication technologies (ICT). The study examines key international instruments and organizations addressing cyberneurosecurity issues. The author proposes specific areas for improving international legal regulation of cyberneurosecurity.

Key words: Cyberneurosecurity, artificial intelligence, cyberthreats, neurotechnology.

Концепция кибернейробезопасности. Стремительный прогресс, достигнутый в области нейротехнологий за последнее десятилетие, служит основанием для больших ожиданий и серьезных опасений. В области нейротехнологий существует множество устройств, имплантированных или внешних, которые, отчасти из-за слабых стандартов шифрования и безопасности, могут быть скомпрометированы в ущерб здоровью пациентов и их правам или даже в ущерб безопасности всего медицинского учреждения [9]. Это может включать такие случаи, как захват протезов конечностей для нанесения ущерба или ограничения подвижности инвалида, вредоносное программирование нейростимуляционной терапии для причинения вреда пациенту, прослушивание сигналов мозгового имплантата для раскрытия личной информации.

Как отмечают Лив Н. и Гринбаум Д., возможно это уже привело к появлению новой области в сфере кибербезопасности – кибернейробезопасности [7].

Международное регулирование. В Концептуальной записке «Новая повестка дня для мира», связанной с Саммитом будущего, отмечалось, что Действие 11 (Не допускать превращения новых сфер в поле боя и содействовать ответственным инновациям) включает разработку мер по устранению рисков, связанных с применяемыми в военной сфере биотехнологий и технологий усиления способностей человека, и в том числе изучение потенциальных последствий достижений в области нейробиологии и развития связанных с ней конвергентных технологий [4].

В июле 2025 года Генеральный секретарь ООН в своем докладе, посвященной достижениям в области науки и техники, особо отметил, что разработки в области биоинспирированной нанофлюидной ионтроники, которая позволяет имитировать некоторые функциональные возможности мозга, такие как обработка сигналов и передача информации, ведут к прогрессу в таких областях, как нейроинспирированные устройства и мозгоподобные вычисления, что потребует тщательной оценки опасности «непреднамеренного и потенциально враждебного применения таких технологий» [1].

В Организации Объединенных Наций многосторонние обсуждения, касающиеся нейротехнологий, управления ими и управления связанными с ними рисками, в основном сосредоточены на трех основных форумах: Совете по правам человека, который изучает последствия нейротехнологий для прав человека, Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), которая сосредоточивает свои усилия на этике нейротехнологий [13]; Института Организации Объединённых Наций по исследованию проблем разоружения (ЮНИДИР), который рассматривает использование нейротехнологий в военных целях и как угроза международному миру и безопасности.

Как отмечается в Докладе ЮНИДИР, исследования кибербезопасности нейротехнологий в контексте вредоносной деятельности в сфере ИКТ и более широких международных дискуссий об управлении ИКТ до сих пор не проводилось [10]. Кроме того, использование нейротехнологий может повлиять на и без того сложные аспекты текущих дискуссий в Группе правительственных экспертов по летальным автономным системам оружия, дискуссий по вопросам разоружения в рамках Конвенции о запрещении биологического и токсинного оружия и Конвенции о запрещении химического оружия.

На сегодняшний день обязательные нормы в сфере вредоносной ИКТ-деятельности закреплены в Конвенции ООН против киберпреступности [3], однако тот факт, что «нейротехнологический» фактор не учитывался при его разработке, делает его недостаточным

для обеспечения кибернейробезопасности. Это требует решения вопроса о необходимости нормативного регулирования в сфере кибернейробезопасности. Так, в Совете Безопасности в рамках брифинга, организованной Швейцарией, была отмечена, что использование достижений нейронауки и нейротехнологий в войне могут значительно повлиять на мир и безопасность, поскольку это ставит важные вопросы о том, как обеспечить применимость Женевских конвенций [5]. Помимо этого, в своем докладе Совет по правам человека призвал определить стандарты, направленные на ограничение видов использования, противоречащих международному праву, включая международное право прав человека и международное гуманитарное право [2].

Региональные инициативы. В рамках региональных и транснациональных организации также было предпринято множество усилий. В частности, Организацией экономического сотрудничества и развития (ОЭСР) приняла Рекомендацию по инновациям в области нейротехнологий [12], Организаций американских государств (ОАГ) − Межамериканскую декларацию принципов в области нейронауки, нейротехнологий и прав человека [8], Глобальная ассамблея по вопросам неприкосновенности частной жизни − Резолюцию о принципах обработки персональных данных в области нейронауки и нейротехнологий [14]. Некоторые исследователи, отмечают [11], что законодательство ЕС, в частности положения Общего регламента по защите данных (GDPR) и Закона ЕС о кибербезопасности, применяют в отношении нейротехнологий при условии их надлежащего толкования и применения.

Несмотря на то, что многие из них касаются прав человека [6], в этих документах также рассматриваются риски и угрозы нейротехнологий, что непосредственно относится к кибернейробезопасности.

Заключение. Таким образом, в международном праве вопросам кибернейробезопасности уделяется ограниченное внимание, поскольку они в основном рассматриваются через призму новых прав человека и этики. Международные и региональные организации в общем признают существование проблемы, но еще не достигли консенсуса по нормативным рамкам. Такие международные организации, как Совет по правам человека, ЮНЕСКО, ЮНИДИР, опубликовали доклады и руководящие документы, подчеркивающие важность кибернейробезопасности. В отсутствие нормативных рамок понимание кибернейробезопасности в настоящее время формируется академическим дискурсом и актами мягкого права от отдельных международных и региональных организаций, которые начали сотрудничать с научными сообществами для повышения осведомленности.

В качестве возможного решения могло бы стать уточнение концепции кибернейробезопасности посредством обмена опытом между государствами и рассмотрение

кибернейробезопасности в рамках отдельного трека Глобального механизма, занимающийся разработками в области ИКТ в контексте международной безопасности и способствующей ответственному поведению государств при использовании ИКТ.

Список источников и литературы:

1. Доклад Генерального секретаря «Последние достижения в области науки и техники и их потенциальное воздействие на усилия в области международной безопасности и разоружения». Док. ООН A/80/237. 22 июля 2025 г. П. 34.
2. Доклад Консультативного комитета Совета по правам человека «Воздействие, возможности и проблемы применения нейротехнологии в отношении поощрения и защиты всех прав человека». Док. ООН. A/HRC/57/61. 8 августа 2025 г. П. 51.
3. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Док. ООН A/RES/79/243. 24 декабря 2024 г.
4. Концептуальная записка № 9 для «Нашей общей повестки дня» [Электронный ресурс] // UNDOCS. URL: https://www.un.org/sites/un2.un.org/files/ our-common-agenda-policy-brief-new-agenda-for-peace-ru.pdf (дата обращения: 31.10.2025)
5. Briefing: Anticipating the impact of scientific developments on international peace and security [Электронный ресурс] // A Plus For Peace. URL: https://www.aplusforpeace.ch/briefing-anticipating-impact-scientific-developments-international-peace-and-security (date of access: 09.11.2025).
6. Bublitz J.C. What an International Declaration on Neurotechnologies and Human Rights Could Look like: Ideas, Suggestions, Desiderata // The American Journal of Bioethics. Neuroscience. 2023. Vol. 15. Iss. 2. P. 96-112.
7. Dubljevic V., Coin A. Policy, Identity, and Neurotechnology: The Neuroethics of Brain-Computer Interfaces. Springer. 2023. 283 p.
8. Inter-American declaration of principles regarding neuroscience, neurotechnologies, and human rights [Electronic resource] // Inter-American Juridical Committee (CJI). URL: https://www.oas.org/en/sla/iajc/themes_recently_concluded_ Neuroscience_neurotechnologies_and_human_rights.asp (date of access: 09.11.2025).
9. Kritika E. Ethical Frontiers: Navigating the Intersection of Neurotechnology and Cybersecurity // Journal of Experimental Neurology. 2025. Vol. 6. Iss. 1. P. 21-25.

10. Mantellassi F., Madziwa E. Neurotechnology in the Military Domain: A Primer. [Electronic resource] // UNIDIR. – URL: (date of access: 09.11.2025).
11. Rainey S., McGillivray K., Akintoye S., Fothergill T., Bublitz C., Stahl B. Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology? // Journal of Law and the Biosciences. 2020. Vol. 7. Iss. 1. P. 1-19.
12. Recommendation of the Council on Responsible Innovation in Neurotechnology [Electronic resource] // OECD Legal Instruments. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0457 (date of access: 09.11.2025).
13. Recommendation on the Ethics of Neurotechnology: working document as of 27 August 2024 [Electronic resource] // UNESDOCS. URL: https://unesdoc.unesco.org/ark:/48223/pf0000391074 (date of access: 09.11.2025).
14. Resolution on principles regarding the processing of personal information in neuroscience. [Electronic resource] // Global Privacy Assembly. URL: https://globalprivacyassembly.com/wp-content/uploads/2024/11/Resolution-on-Neurotechnologies.pdf (date of access: 09.11.2025).

Наталья Сергеевна Глебова,
Студент 3 курса бакалавриата кафедры политологии, института международных отношений и социально-политических наук, Московский государственный лингвистический университет «МГЛУ»
E-mail: naty.glebova@gmail.com

Natalia S. Glebova,
Third-year Bachelor student, Department of Political Science, Institute of International Relations and Social and Political Sciences, Moscow State Linguistic University "MSLU"
E-mail: naty.glebova@gmail.com

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ НА ПРИМЕРЕ ОРГАНИЗАЦИИ АМЕРИКАНСКИХ ГОСУДАРСТВ

THE FIGHT AGAINST CYBERCRIME ON THE EXAMPLE OF THE ORGANIZATION OF AMERICAN STATES

Аннотация. На основе американского опыта можно выявить такие успешные меры борьбы против киберпреступности, как принятие стратегических документов, обеспечение постоянного мониторинга информации и обмена разведданными о новых угрозах, информирование общества, тесное взаимодействие с правоохранительными органами и международными партнерами, что впоследствии позволяет успешно противодействовать преступным группировкам и их атакам. Не последнюю роль играет сотрудничество через региональную сеть CSIRTAmericas, которая объединяет национальные и секторальные CSIRTs. Таким образом, изучение опыта Организации американских государств является полезным в исследовании данной проблематики.

Ключевые слова: киберпреступность, региональное объединение, стратегические национальные документы по кибербезопасности, CSIRT, борьба с кибертерроризмом, Организация американских государств.

Abstract. Based on the American experience, such efficient measures for combat against cybercrime as the adoption of strategic documents, ensuring constant information monitoring and intelligence sharing about new threats, public awareness campaigns, close cooperation with law enforcement agencies and international partners can be identified. This comprehensive approach subsequently enables successful counteraction against criminal groups and their attacks. Cooperation through the regional CSIRTAmericas network, which unites national and sectoral CSIRTs, also plays a significant role. Thus, studying the experience of the Organization of American States is useful while researching this problem area.

Key words: cybercrime, regional association, national cybersecurity strategic documents, CSIRT, countering cyberterrorism, Organization of American States.

Текущий доклад стремится осветить опыт обеспечения информационной безопасности на основе американских государств, в частности, стран-членов Организации американских государств (далее – ОАГ).

CSIRT как эффективный метод реагирования на угрозы. Одним из первых крупномасштабных компьютерных инцидентов, обративших всеобщее внимание на кибертерроризм, стал так называемый червь Морриса, побудивший властей США создать центральную компанию, способную реагировать на последующие угрозы такого типа [2; 5]. После этого случая набирает популярность уже существовавший до этого термин CSIRT, или же группа (команда) реагирования на компьютерные инциденты безопасности. Такие команды предоставляют набор как превентивных, так и, например, реактивных услуг, куда входит обмен информацией, отслеживание кибератак, управление уязвимостями в системах и повышение общего уровня осведомленности. Такие группы часто спонсируются и продвигаются государственными структурами. Примерами являются существующие на данный момент CSIRTs в Латинской Америке, большая часть которых находятся при министерствах, ответственных за научную деятельность или же имеющих отношение к развитию технологий (ColCERT при Министерстве информационных технологий в Колумбии), помимо них есть также команды, подведомственные кабинету президента (CTIR Gov в Бразилии). Немало и групп при министерстве обороны, что подчеркивает стратегически важный характер обеспечения информационной безопасности на уровне государства [4].

В 2023 году на официальном сайте ОАГ был выложен документ «Practical guide for CSIRTS» (перевод на рус.: «Практическое руководство к CSIRTS») [4], в котором подробно описывается деятельность команд реагирования на уровне государств Латинской Америки. ОАГ активно поощряет создание данных организаций и поддерживает их деятельность, более того, она также даёт собственную оценку эффективности данных команд, не исключая того, что некоторые примеры создания CSIRT фактически не способствуют поддержанию информационной безопасности. Вместе с тем ОАГ даёт краткие рекомендации к созданию CSIRT на основе модели устойчивого бизнеса, используя технологию CANVAS – модель, используемая при основании бизнес-компаний и включающая в себе несколько этапов. Сюда входит определение целевой аудитории (к примеру, государственные органы или же частный сектор), выстраивание ценностного предложения (предотвращение, реагирование, обнаружение, реагирование на инциденты), определение каналов взаимодействия (веб-сайты, социальные сети

и прочие цифровые платформы), привлечение партнёров (это могут быть любые заинтересованные стороны, включая университеты, правоохранительные органы или даже международные организации). Так, авторы руководства уверены, что следование этим этапам способствует достижению эффективного результата. Более того, в целях регионального транснационального сотрудничества была создана сеть CSIRTAmericas, которая обеспечивает обмен разведданными об угрозах, связанных с кибербезопасностью, между 29 CSIRTs из 20 государств ОАГ [4].

Программа ОАГ по кибербезопасности. В 2016 году Организацией американских государств была принята программа по кибербезопасности [1], целью которой было создание открытого, безопасного и устойчивого цифрового пространства для всего западного полушария. Программа гарантировала обеспечить тесное сотрудничество и эффективный и своевременный обмен информацией на национальном, региональном и транснациональном уровнях для предотвращения новых угроз, обязывалась обозначить проблему и повысить осведомлённость граждан об исходящих рисках виртуального пространства, а также помочь странам-участницам ОАГ поддерживать высокий уровень информационной безопасности и отвечать на предстоящие вызовы. Причём совместные усилия должны предприниматься не только в качестве превентивных мер, но и для восстановления того или иного пострадавшего члена объединения от нанесённого киберпреступниками ущерба. Что касается деятельности ОАГ по выполнению вышеперечисленных целей, то программа предложила три основные траектории: прежде всего, она настаивает на разработке членами организации национальных стратегических документов по кибербезопасности, которые включают всех соответствующих заинтересованных сторон и адаптированы к законодательной, культурной, экономической и структурной ситуации каждой страны. Следующей траекторией является помощь в создании государствами CSIRTs и в предоставлении индивидуальной технической помощи и возможности для обучения с целью укрепления национальных институтов и организаций. Наконец, программа подчёркивает важность проведения большего числа научных исследований по теме и повышения осведомлённости населения. Так, программа предлагает разработку технических документов и написание отчётов для политических лидеров, руководителей частных и государственных организаций, а также гражданского общества с целью обратить внимание на ключевые события, вопросы и проблемы кибербезопасности в регионе [1].

Благодаря эффективной деятельности ОАГ был совершен значительный скачок в обеспечении информационной безопасности несмотря на то, что общее состояние развития данной области в странах ОАГ (в частности, Латинской Америки и Карибского бассейна) характеризуется низким уровнем защищённости от киберугроз. Тем не менее, следует выделить

такие положительные результаты, как разработка более 17 национальных стратегических документов по кибербезопасности (о которых ещё пойдёт речь ниже) [3], успешное обучение более 15 000 граждан противостоянию кибертерроризму с высоким показателем осведомлённости в области кибербезопасности и цифровой дипломатии, выпуск региональных докладов о состоянии безопасности информационного поля в странах-членах ОАГ, а также публикация множества докладов и исследований по соответствующей тематике. Более того, ОАГ прилагает усилия не только в борьбе с терроризмом, но еще и уделяет внимание гендерному неравенству, посвятив проблеме цифрового терроризма отдельный документ с учетом гендерной проблематики. Так, еще одним важным результатом деятельности ОАГ является просвещение женщин в область кибербезопасности и проведение специальных тренингов, чтобы обучить их защищать себя.

Опыт разработки стратегий национальной кибербезопасности. Благодаря анализу стратегий национальной безопасности (далее – НКС) мы можем выявить ряд универсальных тенденций и особенностей, сформировавшие современный ландшафт цифровой безопасности. Во-первых, стоит отметить, что для всех стран проблема кибербезопасности стала стратегическим приоритетом и неразрывно связана с экономическим развитием, национальной безопасностью и защитой прав граждан [3]. Из общих трендов можно выделить то, что по большей части стратегии сходятся в целях и стремятся развить кадровый потенциал, предоставить правовую базу и защитить критическую инфраструктуру. Тем не менее, пути достижения этих целей отличаются так же, как и те отрасли, на которых в каждой стране делается акцент. К примеру, можно определить следующую закономерность: страны Карибского бассейна часто рассматривают цифровую безопасность через призму экономической стабильности. Примерами таких стран являются Ямайка и Тринидад и Тобаго. Страны же Южной Америки в основном делают упор на национальную безопасность и противодействие транснациональной киберпреступности. Особую позицию занимают государства Центральной Америки, включая Коста-Рику и Панаму, которые стараются найти баланс между получением экономических выгод от цифровизации и необходимостью обеспечения надежности информационных систем [3].

Исследование, проведённое экспертами ОАГ, выявило, что самым значимым фактором при разработке успешных стратегических документов было применение многостороннего подхода. Из этого следует, что значительно больше шансов на реализацию своих стратегий имели те страны, которые активно вовлекали в разработку документа различные группы заинтересованных лиц, включая научные сообщества, институты, гражданское общество, частный сектор и так далее, что привело не только к созданию сбалансированного документа, но и сформировало чувство сопричастности разных социальных групп людей. По мнению ученых

именно это чувство совместной разработки документа способствовало получению необходимой поддержки со стороны населения для дальнейшего воплощения её в жизнь.

Другим важным фактором является назначение конкретного органа, который наделяется соответствующими полномочиями и ресурсами для реализации стратегии. Ярким примером здесь становится Уругвай, поскольку за координацию выполнения национальной цифровой повестки стоит Агентство электронного правительства и информационного общества (AGESIC), которое подчиняется непосредственно президенту страны [3].

При этом нельзя забывать, что современный мир изменчив, и государства встречаются с новыми вызовами, к которым нужно уметь своевременно адаптироваться. Из этого следует, что все стратегии должны были пересмотрены и актуализированы в соответствии с новыми опасностями и угрозами.

Заключение. XXI принёс с собой новые вызовы мировому сообществу, которые представляют существенную опасность устоявшейся системе и не должны быть проигнорированы. Напротив, государства должны приложить совместные усилия с целью противостоять новым угрозам. В данном контексте отличным примером совместной работы по борьбе с киберпреступностью и защитой цифрового пространства является Организация американских государств, которая активно разрабатывает документы и стратегии для обеспечения безопасности региона. Организация непрерывно работает над улучшением состояния цифровой безопасности всего региона, демонстрируя положительные результаты своей деятельности. Автор считает, что данный опыт следует быть учтен Российской Федерацией при пересмотре существующих стратегий и разработке новых документов в области информационной безопасности.

Список источников и литературы:

1. CICTE’s Cybersecurity Program / Org. of American States (OAS). – 2016.
2. Countering Ransomware Financing [Electronic resource] / FATF. – Paris : FATF, 2023. – URL: http://www.fatf-gafi.org/publications/Methodsandtrends/countering-ransomware-financing.html (дата обращения: 08.11.2025).
3. National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions / Org. of American States (OAS). – 2022.
4. Practical Guide for CSIRTs (Volume 2): A Sustainable Business Model / Organization of American States (OAS). – 2023.
5. Tanczer L. M. CSIRTs and global cybersecurity: how technical experts support science diplomacy / L. M. Tanczer, I. Brass, M. Carr // Global Policy. – 2018.

Елена Евгеньевна Гуляева,
к.ю.н., доцент кафедры международного права,
Дипломатическая академия МИД России,
E-mail: gulya-eva@yandex.ru

Elena E. Gulyaeva,
Candidate of Legal Sciences, Department of International Law,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: gulya-eva@yandex.ru

ЗАЩИТА ТРАДИЦИОННЫХ ЦЕННОСТЕЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ БРАЗИЛИИ

PROTECTING TRADITIONAL VALUES IN BRAZIL’S DIGITAL SPACE

Аннотация. Автором раскрыта особенность защиты традиционных ценностей в цифровом пространстве Бразилии. Криминализация определённых видов поведения в киберпространстве отражает как защиту основополагающих прав, так и стремление государства поддерживать определённый нравственный и социальный порядок в цифровой среде. Конституционное измерение цифрового уголовного права не ограничивается защитой индивидуальных прав, но оно распространяется на защиту общественного порядка и коллективных нематериальных правовых благ, таких как социальное доверие, целостность общественных дискуссий и информационная безопасность.

Ключевые слова: уголовная политика, цифровое право, традиционные ценности, права человека, киберпреступность, право на неприкосновенность частной жизни.

Abstract. The author reveals the specific nature of protecting traditional values in Brazil's digital space. Criminalizing certain types of behavior in cyberspace reflects both the protection of fundamental rights and the state's desire to maintain a certain moral and social order in the digital environment. The constitutional dimension of digital criminal law is not limited to the protection of individual rights but extends to the protection of public order and collective intangible legal assets, such as social trust, the integrity of public debate, and information security.

Key words: criminal policy, digital law, traditional values, human rights, cybercrime, right to privacy.

Бразильскую уголовную политику в отношении киберпреступности нельзя рассматривать исключительно как ответ на угрозы, возникающие в результате использования цифровых технологий. Правовая база в области обеспечения цифровой безопасности основана на конституционных принципах и защите традиционных ценностей. В этом смысле криминализация определённых видов поведения в киберпространстве

отражает как защиту основополагающих прав, так и стремление государства поддерживать определённый нравственный и социальный порядок в цифровой среде. Так, статья 5 Федеральной конституции Бразилии 1988 года закрепляет основные права – право на неприкосновенность частной жизни, право на частную жизнь, защиту чести и достоинства [1].

Криминализация таких деяний, как несанкционированный доступ к компьютерным устройствам, несанкционированное распространение личного контента или кража цифровых персональных данных, отвечает не только необходимости предотвращения финансовых потерь, но и необходимости защиты человеческого достоинства как высшей ценности конституционного строя. Таким образом, защита чести и неприкосновенность частной жизни рассматриваются как нематериальные права, защита которых оправдана их тесной связью с личной автономией, свободным развитием личности и экзистенциальной сферой индивида в киберпространстве.

По мнению профессора Донеды [2], защита персональных данных является конкретным продолжением права на неприкосновенность частной жизни и представляет собой неотъемлемый элемент обеспечения информационного самоопределения личности. По его словам, «контроль над персональными данными представляет собой базовое условие осуществления свободы в обществах, характеризующихся цифровизацией». С этой точки зрения, криминализация поведения, наносящего ущерб частной сфере, вызвана необходимостью защитить сущность человеческой личности от злоупотребления технологиями. Уголовное право, таким образом, становится вспомогательным механизмом защиты, призванным защитить достоинство от непоправимого ущерба, который не могут предотвратить гражданские или административные средства правовой защиты.

Уголовная политика отражает ценностный аспект, связанный с сохранением моральных, этических и семейных ценностей. Законодательный дискурс систематически использовал эти элементы не только для оправдания принятых новых законов, но и в качестве содержательной основы для уголовно-правового вмешательства. В частности, защита детей и подростков от материалов, содержащих насилие, сексуальные или разжигающие ненависть материалы, представлялась как продолжение конституционной обязанности государства обеспечивать всестороннее развитие личности и укреплять семью как основное пространство социализации.

Эта аксиологическая структура особенно ярко проявляется в недавно принятых законах, таких как Закон № 15.211/2025 (Статут о детях и подростках – цифровая инфраструктура) [3], который требует от цифровых платформ внедрения механизмов проверки возраста, родительского контроля и удаления вредоносного контента. Заявленная

цель этих положений выходит за рамки простого предотвращения преступлений: она направлена на защиту детей, сохранение семьи и обеспечение того, чтобы цифровая среда не подрывала ценности, считающиеся основополагающими для социальной сплоченности. Данная законодательная стратегия, хотя и подвергается критике со стороны некоторых ученых, предупреждающих об опасности моральной инструментализации уголовного права, демонстрирует тенденцию к использованию права как средства укрепления традиционных этических принципов перед лицом вызовов цифровой современности.

Судья Баррозу [4] анализирует противоречие между свободой выражения мнений и правами личности. По мнению автора, конституционное право Бразилии требует баланса, который «гармонизирует право на выражение идей с необходимостью защиты чести, неприкосновенности частной жизни и семейной жизни». В цифровой сфере такая гармонизация подразумевает разработку правовых механизмов, предотвращающих частную цензуру со стороны технологических компаний, не умаляя при этом эффективной защитой основных прав, особенно когда речь идет о психологическом и нравственном развитии несовершеннолетних.

В этом ключе цифровое уголовное право приобретает символическую функцию: подтверждает коллективные ценности, такие как солидарность, информационная безопасность и защита семьи как ядра формирования гражданства. Эту функцию следует интерпретировать как «карательный морализм», а именно как стратегию защиты минимальных этических принципов, которые делают демократическую жизнь возможной.

Конституционное измерение цифрового уголовного права не ограничивается защитой индивидуальных прав, но оно распространяется на защиту общественного порядка и коллективных нематериальных правовых благ, таких как социальное доверие, целостность общественных дискуссий и информационная безопасность. Эти активы, хотя и нематериальны, составляют важнейшие основы демократического сосуществования и функционирования верховенства права в цифровую эпоху. Расширение киберпространства экспоненциально увеличило возможности коммуникации, взаимодействия и распространения информации; однако оно также привело к беспрецедентным рискам, таким как скоординированное распространение дезинформации, использование цифровых платформ для идеологической радикализации или разжигания ненависти, а также атаки на критически важную инфраструктуру, поддерживающую основные государственные услуги.

Криминализация таких деяний, как манипулирование данными, киберсаботаж, распространение запрещенной информации или разжигание ненависти, отвечает именно этой логике. В цифровой среде подобные действия не только нарушают индивидуальные

права, такие как право на неприкосновенность частной жизни, честь и репутацию, но и ставят под угрозу коллективное доверие к демократическим институтам и функциональность коммуникационных систем, на которых строится публичная сфера. По мнению судьи Баррозу [4], поддержание свободного, плюралистичного и надежного цифрового пространства является существенным условием эффективного осуществления свободы выражения мнений, поэтому вмешательство государства может быть законным, если оно направлено на сохранение демократического плюрализма в противовес угрозам, искажающим публичные дебаты или подрывающим свободу слова.

В современных условиях, характеризующихся стремительным развитием цифровых технологий, доступом к интернету с раннего возраста и повсеместной распространенностью платформ в повседневной жизни, защита детей и подростков стала одной из важнейших задач конституционного и уголовного права Бразилии. Детство, традиционно считавшееся защищенным этапом развития человека, постепенно включается в цифровую экосистему, порождая новые формы уязвимости, не предусмотренные традиционными правовыми нормами. Одним из наиболее тревожных явлений этой трансформации является так называемое «взросление», понимаемое как преждевременное знакомство детей и подростков с контентом, динамикой, дискурсами, потребительскими практиками и опытом, типичными для мира взрослых, часто опосредованное алгоритмами и стратегиями цифрового маркетинга.

Этот процесс взросления несовершеннолетних не только влияет на психологическое, эмоциональное и социальное развитие несовершеннолетних, но и может поставить под угрозу основные права, закреплённые в Федеральной конституции 1988 года, такие как человеческое достоинство, свободное развитие личности, неприкосновенность частной жизни и право на адекватное образование. В то же время, это ставит государство перед необходимостью переосмыслить свою роль в условиях возникающих в киберпространстве рисков, включая превентивную политику, эффективные механизмы регулирования и способы привлечения к ответственности технологических платформ. Таким образом, комплексная защита детей в цифровой среде не может ограничиваться уголовным преследованием после причинения вреда, а должна включать структурные стратегии, направленные на создание безопасной инклюзивной цифровой среды, учитывающей особые потребности детей и подростков в развитии [1].

Список источников и литературы:

1. Constitución Federal de la República Federativa de Brasil de 1988. Gaceta Oficial de la Unión, Brasilia-DF: Presidencia de la República. Disponible en: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (дата обращения: 22.12.2025).

2. Doneda, D. (2011). La protección de datos personales como un derecho fundamental. Espaço Jurídico Journal of Law, 12(2), 91-108. Disponible en: http://dialnet.unirioja.es/descarga/articulo/4555153.pdf (дата обращения: 22.12.2025).

3. Brasil. (2025). Ley n.º 15.211, de 17 de septiembre de 2025. Establece el Estatuto Digital de Protección de Niños y Adolescentes y otras disposiciones. Gaceta Oficial de la Unión, Brasilia-DF, 18 sep. 2025: Presidencia de la República. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm (дата обращения: 22.12.2025).

4. Barroso, L. R. (2023). Libertad de expresión, prensa y redes sociales. Revista Jurídica de la Presidencia, 25(137), 11-40. Disponible en: http://www.stf.jus.br/arquivo/cms/codi/anexo/LiberdadeExpressao_completo.pdf (дата обращения: 22.12.2025).

Денис Сергеевич Кортунов,
аспирант, ассистент кафедры регионоведения,
международных отношений и политологии
Высшая школа социально-гуманитарных наук
и международной коммуникации,
Северный (Арктический) федеральный университет имени М.В. Ломоносова,
E-mail: d.kortunov@narfu.ru

Denis S. Kortunov,
Postgraduate student, Teaching assistant of the Department of Regional Studies, International Relations and Political Science
Higher School of Social Sciences, Humanities and International Communication,
Northern (Arctic) Federal University named after M.V. Lomonosov,
E-mail: d.kortunov@narfu.ru

ПОДДЕЛЬНЫЕ НОРМАТИВНЫЕ АКТЫ КАК ВЫЗОВ СИСТЕМЕ ПОЛИТИЧЕСКИХ КОММУНИКАЦИЙ И НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

FAKE REGULATIONS AS A CHALLENGE TO THE SYSTEM OF POLITICAL COMMUNICATIONS AND NATIONAL SECURITY OF RUSSIA

Аннотация. В статье рассматривается феномен распространения поддельных нормативных актов как одного из новых инструментов информационно-психологического воздействия, оказывающего влияние на систему политических коммуникаций и национальную безопасность Российской Федерации. Проанализированы масштабы явления, характер угроз, а также предложены меры по противодействию этому виду информационного давления.

Ключевые слова: информационная безопасность, политические коммуникации, фейковые документы, дезинформация, национальная безопасность.

Abstract. The paper examines the phenomenon of the dissemination of fake normative acts as a new instrument of information and psychological influence affecting the system of political communications and the national security of the Russian Federation. The scale of the phenomenon, the nature of threats, and possible countermeasures are analyzed.

Key words: information security, political communications, fake documents, disinformation, national security.

Актуальность вызова. В условиях нарастания геополитической напряженности в мире государства и другие акторы международных отношений активно обращаются к

нетрадиционным, но не менее эффективным инструментам и методам. Сегодня именно информационная среда является новым и уникальным пространством различного рода противостояний. Эффективность применяемых в цифровой среде мер бесспорна в связи с возможностью широкого охвата аудитории и отсутствием каких-либо внушительных материальных затрат. Когда к этому добавляются официальные символы министерств (печати и бланки), а также подписи ответственных должностных лиц, эмоциональный эффект, направленный на пользователя сети Интернет, достигается гораздо быстрее.

В связи с этим одним из качественно новых инструментов информационно-психологического давления стало создание и распространение поддельных нормативных документов: фейковых указов, постановлений, распоряжений и т.д. Поддельные документы представляют собой качественно новый этап информационных манипуляций, цель которых – дестабилизация общественно-политической ситуации и подрыв доверия к органам государственной власти.

Масштабы и характер явления. Аналитики автономной некоммерческой организации «Диалог Регионы» отмечают, что в период с января по сентябрь 2025 года выявлено 182 поддельных документа, а также около 30 тысяч копий этих документов, в то время как в предыдущие годы подобные фейки были единичными [3]. Подчеркивается, что основными темами стали политика, социально-бюджетные меры в контексте специальной военной операции и здравохранение [3].

Так, в качестве примера можно привести распространявшийся в мае 2025 года поддельный указ Президента Российской Федерации о присвоении Республике Дагестан автономного статуса [7]. Цель распространения этого и других подобных фейков очевидна – попытка внести разлад в российское общество на национальной почве. Во время заседания Совета по межнациональным отношениям 5 ноября 2025 года Президент России Владимир Путин отметил, что из-за рубежа постоянно наблюдаются попытки «пошатнуть наше единство» [4].

Создатели фейковых документов в последнее время стараются учитывать региональную специфику. Например, по данным Центра управления регионом Архангельской области, только в данном субъекте за 2025 год было обнаружено четыре уникальных поддельных постановления [9]. Как отмечалось ранее, среди тем фигурирует и сфера здравоохранения. Так, в конце октября 2025 года в тематических телеграм-каналах г. Архангельска распространялось фейковое постановление министерства здравоохранения от 25 октября 2025 года № 15-пз, гласящее, что все лекарства в Архангельской области будут отпускаться только по рецепту. Однако в данном случае создатели фейка допустили ошибку, так как документ якобы подписан региональным министром, который на тот

момент уже находился под стражей. Именно на такие детали стоит обращать внимание пользователю, когда он сталкивается с сомнительным контентом.

Как справедливо отмечает А.В. Манойло, главной задачей информационных войн является разделение и поляризация общества, формирование чувства ненависти и направление потока эмоций против действующей власти [2, с. 102]. Это, в свою очередь, оказывает влияние на систему политических коммуникаций. Провокационное содержимое документов подрывает доверие со стороны граждан к субъектам управления, а также искажает общественное мнение. Кроме того, поскольку основными платформами для распространения являются мессенджеры, практически не поддающиеся государственному регулированию, происходит эрозия цифрового суверенитета.

Угроза национальной безопасности и механизмы противодействия. Россия в стратегических документах осознает опасность текущих тенденций в информационной среде. В Концепции внешней политики Российской Федерации отмечается, что в информационном пространстве на систематической основе развернута антироссийская пропагандистская кампания, включающая дезинформацию, клевету и разжигание ненависти [1]. Соответственно, в рамках внешнеполитического курса России обозначена задача противодействия масштабным информационным атакам, инициированным недружественными странами.

Один из пунктов Стратегии национальной безопасности РФ гласит, что против России проводятся информационные кампании, целью которых является создание негативного образа России [6]. При этом образ России может формироваться как во внешней среде, так и во внутренней, и это следует учитывать, реализуя информационную политику.

Стоит отметить, что у России нет официального документа, который регулировал бы операции в информационном пространстве, в отличие, например, от США, где существует Стратегия ведения операций в информационном пространстве, утвержденная в 2023 году. Целью данного документа является повышение способности использовать информационную мощь для обеспечения комплексного сдерживания, проведения определенных кампаний и создания устойчивых преимуществ от этого использования [10]. Работа по информационному противостоянию и атакам координируется по нескольким линиям в США, среди которых Агентство по глобальным медиа, Центр глобального взаимодействия Госдепартамента, Совместный военный центр информационных операций [8]. Аналогичная деятельность ведется в Европейском союзе (Оперативная группа по стратегическим коммуникациям), и в Североатлантическом альянсе (Передовой центр по вопросам стратегических коммуникаций в Латвии) [8]. Наличие специализированных

подразделений в структурах крупнейших международных институтов свидетельствует о серьёзной институционализации информационных войн.

Наиболее очевидным методом реагирования на информационную перенасыщенность является повышение уровня медиаграмотности населения. Проведение образовательных кампаний, включение в школьные и университетские программы дисциплин, направленных на развитие конкретно критического мышления, а также формирование привычки проверять источники информации – все эти меры могут способствовать формированию устойчивости граждан к информационно деструктивным механизмам без необходимости прибегать к запретам. Кроме того, противодействие информационным атакам не может быть в полной мере эффективным, если этим занимается исключительно государство. Даже при наличии стратегий, правовых механизмов и других решений, их эффективность будет слишком ограниченной, если не будет участия гражданского и научного сообществ. Именно на этом уровне закладываются ценности, формируется навык критического мышления и устойчивость к манипуляциям. В условиях постоянных информационных трансформаций и развития технологий важно действовать гибко, локально и инициативно.

Помимо внутриполитических мер сегодня важно формировать устойчивые платформы для взаимодействия – двусторонние и многосторонние механизмы, направленные на противодействие фейкам и информационным манипуляциям, особенно в сферах, затрагивающих вопросы национальной безопасности. Хорошим примером служит международное взаимодействие в рамках Шанхайской организации сотрудничества. Еще в 2009 году страны-члены ШОС стали одними из первых, кто выступил с инициативой взаимодействия в области информационных технологий и обеспечения международной информационной безопасности, заключив соглашение о сотрудничестве в этой сфере. В документе признаётся, что развитие информационных технологий приводит к появлению новых вызовов и угроз, таких как разработка и применение информационного оружия, подготовка и ведение информационных войн, информационный терроризм, информационная преступность, использование доминирующего положения в киберпространстве в ущерб интересам и безопасности других государств [5]. Также в качестве угрозы отмечается распространение информации, которая может нанести вред общественно-политической, социально-экономической, духовной, нравственной и культурной жизни общества.

Заключение. Таким образом, распространение поддельных нормативных актов представляет себе новый вызов для системы политических коммуникаций и национальной безопасности Российской Федерации. Данное обстоятельство требует системного подхода

к противодействию, включающего как совершенствование регулирования информационного пространства, так и развитие медиаграмотности населения. Немаловажным является развитие международного сотрудничества в области информационной безопасности. Сегодня государствам необходимо не только реагировать на возникающие угрозы, но и выстраивать долгосрочную стратегию формирования устойчивого информационного пространства. Россия делает шаги в этом направлении, однако необходима консолидация усилий государства, науки и общества для более эффективного противодействия информационным атакам.

Список источников и литературы:

1. Концепция внешней политики Российской Федерации (утверждена Указом Президента РФ № 229 от 31 марта 2023 г.) [Электронный ресурс] // Президент России. URL: https://www.scrf.gov.ru/security/international/document25/ (дата обращения: 31.10.2025).
2. Манойло Андрей Викторович. Информационная война и новая политическая реальность (I) [Электронный ресурс] // Российский социально-гуманитарный журнал. 2021. № 1. URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-i-novaya-politicheskaya-realnost-i (дата обращения: 03.11.2025).
3. Рост числа фейковых документов в интернете в России [Электронный ресурс] // Lenta.ru. URL: https://lenta.ru/news/2025/10/14/v-rossii-zafiksirovan-rost-chisla-feykovyh-dokumentov-v-internete/ (дата обращения: 03.11.2025).
4. Сила в единстве [Электронный ресурс] // Российская газета. URL: https://rg.ru/2025/11/05/sila-v-edinstve.html (дата обращения: 05.11.2025).
5. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/902289626 (дата обращения: 03.11.2025).
6. Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента РФ № 400 от 2 июля 2021 г.) [Электронный ресурс] // Президент России. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 31.10.2025).
7. Фейк: указом Владимира Путина Республике Дагестан присвоен статус автономной [Электронный ресурс] // Война с фейками. URL: https://www.войнасфейками.рф/common/fejk-ukazom-vladimira-putina-respublike-dagestan-prisvoen-status-avtonomnoj/ (дата обращения: 03.11.2025).
8. Фейковые новости столь же опасны, как и ядерное оружие [Электронный ресурс] // Республиканское информационное агентство «Кабардино-Балкария». URL: https://kbrria.ru/000v-mire-novostey/Feykovyenovostistolzheopasnykakiyadernoeoruzhie (дата обращения: 07.11.2025).
9. Центр управления регионом Архангельской области: опровержение поддельных постановлений [Электронный ресурс] // VK.com. URL: https://vk.com/wall-201474339_8693 (дата обращения: 05.11.2025).
10. Strategy for Operations in the Information Environment [Electronic resource] // U.S. Department of Defense. URL: https://goo.su/NUlSkm (date of access: 27.11.2025).

Софья Александровна Мисаревич,
Студент ФГБОУ ВО «КНИТУ»
Казань, Россия
Научный руководитель: Шевко Наиля Рашидовна,
кандидат экономических наук, доцент,
доцент кафедры «Информационная безопасность»
E-mail: sony394sever@mail.ru

Sofya A. Misarevich,
Student of Kazan National Research Technological University (KNRTU)
Kazan, Russia
Scientific supervisor: Shevko Nailya Rashidovna,
Candidate of Economic Sciences, Associate Professor,
Associate Professor of the Department of Information Security
E-mail: sony394sever@mail.ru

ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ: ЗАЩИТА ПРАВ ГРАЖДАН И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

LEGAL RISKS OF USING BIOMETRIC DATA: PROTECTING CITIZEN'S RIGHTS AND ENSURING SECURITY

Аннотация: в данной статье проводится анализ правовых рисков использования биометрических данных в РФ, выявление системных пробелов в законодательстве. В качестве решения предлагается использование триединого подхода: законодательное уточнение, технологическая защита и просветительская работа.

Ключевые слова: биометрические данные, правовые риски, Единая биометрическая система (ЕБС), цифровая идентичность, безопасность информации.

Abstract: this article analyzes the legal risks of using biometric data in the Russian Federation and identifies systemic gaps in legislation. A three-pronged approach is proposed as a solution: legislative clarification, technological protection, and educational work.

Key words: biometric data, legal risks, Unified Biometric System (UBS), digital identity, information security.

Современный этап развития общества, характеризуемый как «эпоха цифровой трансформации», принес с собой не только беспрецедентные технологические возможности, но и новые, сложные вызовы в сфере защиты прав личности. Одной из наиболее чувствительных и дискуссионных областей стало использование биометрических данных – уникальных физиологических или поведенческих характеристик человека, таких

как отпечатки пальцев, рисунок радужной оболочки глаза, геометрия лица, голос и др. Широкое внедрение биометрии в системы идентификации и аутентификации, от разблокировки смартфонов до контроля доступа на объекты и в государственные цифровые сервисы, кардинально меняет парадигму взаимодействия между человеком, технологией и государством. Ключевыми задачами статьи являются комплексный анализ правовых рисков, связанных с обработкой биометрических данных, оценка адекватности существующего правового регулирования в России для защиты прав граждан и обеспечения безопасности, а также выработка конкретных предложений по совершенствованию законодательства и правоприменительной практики.

Актуальность. Биометрические технологии стали массовыми, используясь в банковском обслуживании, на транспорте, в социальных сетях и на рабочих местах. В отличие от пароля или PIN-кода, который можно изменить в случае утечки, биометрические данные не подлежат замене. Компрометация отпечатка пальца или скана лица означает его необратимую утрату в качестве надежного идентификатора на всю жизнь человека, порождая долгосрочные и непредсказуемые риски. Биометрические данные не просто идентифицируют человека – они являются неотъемлемой частью его биологической сущности. К сожалению, их обработка и хранение осуществляется также, как и обычных сведений, без обеспечения надлежащего уровня безопасности.

Статистические данные. В период с января по июль 2025 года с помощью Единой биометрической системы было оказано 5,9 млн услуг, связанных с биометрическими данными. В данную статистику включены данные сервисов самой ЕБС. За январь 2025 года было оказано 930 тысяч услуг. К июлю 2025 года их число выросло до 5,9 млн. Необходимо учесть, что статистика охватывает только транзакционные сервисы, реализованные при поддержке Министерства цифрового развития, связи и массовых коммуникаций РФ. [4]

Правовое регулирование в РФ.

Правовой основой защиты биометрических данных являются:

– статья 272.1 УК РФ («Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения»); [8]

– статья 13.11.3 КоАП РФ («Нарушение требований в области размещения и обработки биометрических персональных данных в государственной информационной системе "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных", иных информационных системах, обеспечивающих аутентификацию на основе биометрических персональных данных

физических лиц»). По данной статье привлекаются операторы, которые обрабатывают биометрию без надлежащего согласия или не обеспечивают должный уровень защиты. [7]

Прямая квалификация преступлений, связанных именно с кражей или неправомерным использованием биометрии, затруднена. На практике такие случаи часто подпадают под ст. 272 УК РФ. Ярких громких дел, связанных именно с ЕБС, пока нет, что может говорить как об отсутствии инцидентов, так и о сложностях в выявлении и квалификации.

Единственный пример инцидента произошел в октябре 2019 года в банке «Сбербанк». На черном рынке продавался архив аудиозаписей разговоров клиентов банка с техподдержкой банка. Таким образом, в сети оказались образцы голосов клиентов банка. Данный инцидент можно отнести к утечке БПД, так как речь также относится к биометрическим данным. [5]

Правоприменительная практика свидетельствует о всестороннем характере защиты информации: спектр мер охватывает как уголовную ответственность за тяжкие деяния, так и административное воздействие при менее опасных нарушениях.

Пробелы и коллизии в законодательстве. Несмотря на наличие правовых норм, действующее законодательство содержит ряд существенных пробелов и коллизий, создающих правовые риски:

− фиктивность «добровольного согласия», закон требует письменного согласия, но на практике оно часто становится условием оказания услуги (банковский кредит, доступ на работу). Гражданин де-факто лишен свободы выбора, что делает его согласие вынужденным и недобровольным по своей сути;

− уязвимость централизованной системы, создание централизованных баз данных, таких как ЕБС, создает крайне привлекательную цель для кибератак. Успешный взлом такой системы приведет к компрометации неизменяемых биометрических данных миллионов граждан. В отличие от пароля, отпечаток пальца или изображение лица невозможно поменять;

− отсутствие цифровой грамотности граждан, подавляющее большинство граждан нашей страны не осознает ценность и риски, связанные с их биометрическими данными. Они не понимают, что это уникальный и неизменный цифровой идентификатор, утеря которого имеет необратимые последствия.

Предложения по усовершенствованию законодательства.

− законодательно закрепить перечень услуг, для которых обязательно использование БПД, и тех, где это использование рекомендовано (желательно) как опция. Также при

запросе таких данных ввести обязательное уведомление и разъяснение гражданам для чего нужен такой тип данных, как и когда можно отозвать согласие на их обработку без потерь;

− создать простой и доступный для всех граждан механизм отзыва согласия с гарантией сохранения базовых прав и услуг;

− перейти от единой базы хранения данных к распределенной архитектуре, где данные хранятся фрагментально и зашифрованы у разных операторов;

− создать регулирующий правила хранения и передачи БПД нормативно-правовой документ, в котором будут прописаны обязательные средства защиты такого типа данных. Ввести обязательное использование шифрование, с использованием отечественных криптографических алгоритмов, проведение регулярного аудита безопасности ЕБС;

− создание и распространение цифрового контента, с помощью которого будет происходить информирование граждан о важности сохранения своих биометрических данных, особенно среди молодежи и пенсионеров.

Заключение. Проведённый анализ выявляет системный характер проблем в сфере правового регулирования биометрических персональных данных (БПД) в Российской Федерации. Несмотря на наличие базового законодательства, его реализация на практике сталкивается с существенными пробелами и коллизиями. Дальнейшее развитие нормативного регулирования в этой сфере должно опираться на триединый подход: законодательное уточнение, технологическая защита и просветительская работа. Только при условии комплексного решения обозначенных проблем возможно обеспечить баланс между инновационным развитием цифровых сервисов и защитой конституционных прав граждан на неприкосновенность частной жизни.

Список источников и литературы:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Федеральный закон от 29 декабря 2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты РФ».

3. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

4. Минцифры РФ зафиксировало пятикратный рост использования ЕБС в первые 6 месяцев 2025 года [Электронный ресурс] // Хабр. 2024. 30 июля. URL: https://habr.com/ru/news/932402/?ysclid=mghbstqql5671406836 (дата обращения: 05.11.2025).

5. Анна Вичугова. Как потерять лицо: утечки биометрических данных – новая угроза Big Data систем [Электронный ресурс] // Big Data School : блог. 2020. 18 января. URL: https://bigdataschool.ru/blog/biometrics-cybersecurity-big-data-leaks/ (дата обращения: 05.11.2025).

6. Единая биометрическая система [Электронный ресурс] // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: официальный сайт. URL: https://digital.gov.ru/activity/czifrovaya-identifikacziya/edinaya-biometricheskaya-systema (дата обращения: 05.11.2025).

7. КонсультантПлюс. КоАП РФ Статья 13.11.3. Нарушение требований в области размещения и обработки биометрических персональных данных в государственной информационной системе "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных", иных информационных системах, обеспечивающих аутентификацию на основе биометрических персональных данных физических лиц [Электронный ресурс] // КонсультантПлюс: электронная база правовых документов. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_34661/a7bb4968db0ef8eefddb5a87fdbc8a6f8d01372f/ (дата обращения: 05.11.2025).

8. КонсультантПлюс. УК РФ Статья 272.1. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения [Электронный ресурс] // КонсультантПлюс: электронная база правовых документов. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/deefead19003ba8266e85fbf42fc31f60ed3c698/ (дата обращения: 05.11.2025).

9. Н. Р. Шевко, С. Я. Казанцев, Э. Н. Хисамутдинова, Проблемы противодействия киберпреступности в современных условиях [Электронный ресурс] // Киберленика – Режим доступа: https://cyberleninka.ru/article/n/problemy-protivodeystviya-kiberprestupnosti-v-sovremennyh-usloviyah/viewer (дата обращения: 05.11.2025).

Федор Васильевич Ниточкин,
Аспирант МГЮА им. О.Е.Кутафина, советник ФКУ «Аппарат Общественной палаты России», ответственный секретарь Координационного совета по общественному контролю за голосованием при Общественной палате Российской Федерации;
E-mail: nitochkin@oprf.ru

Fedor V. Nitochkin,
Kutafin Moscow State Law University (MSAL), postgraduate student. Executive office of the Civic Chamber of the Russian Federation, executive secretary of the Coordinating council for public control over voting, Moscow,
E-mail: nitochkin@oprf.ru

ЛЕГИТИМНОСТЬ ВЛАСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

LEGITIMACY OF POWER IN THE CONTEXT OF DIGITALIZATION OF STATE AND MUNICIPAL ADMINISTRATION

Аннотация. В статье анализируются перспективы внедрения механизмов регулярной оценки гражданами эффективности деятельности должностных лиц через единую цифровую платформу в контексте реализации Указа Президента Российской Федерации о национальных целях развития. Рассматриваются правовые основы, возможные критерии оценки, а также потенциал такого механизма для преодоления кризиса представительной демократии и совершенствования механизма легитимации государственной власти.

Ключевые слова: цифровая трансформация, оценка эффективности, обратная связь, легитимность власти, представительная демократия, ключевые показатели эффективности, общественный контроль.

Abstract. The article analyzes the prospects for implementing mechanisms for regular assessment by citizens of the effectiveness of public officials through a unified digital platform in the context of implementing the Presidential Decree on national development goals. The legal framework, possible evaluation criteria, and the potential of such a mechanism to overcome the crisis of representative democracy and strengthen the legitimacy of power are considered.

Key words: digital transformation, performance evaluation, feedback, legitimacy of power, representative democracy, key performance indicators, public control.

Цифровые технологии и преодоление кризиса представительной демократии. Кризис представительной демократии, который мы наблюдаем в современном мире, связан

с падением доверия граждан к властным институтам, их (само)отстранением от влияния на принимаемые решения [9, 10]. Как отмечают эксперты происходит устаревание самой модели представительной демократии, которая основывается на делегировании гражданами властных полномочий своим представителям в условиях неэффективности обратной связи и отсутствия (или деградации) института политической ответственности [8].

Одновременно с этим, наблюдается взрывной рост использования цифровых технологий в сфере государственного и муниципального управления, что не может не сказываться на развитии местной инициативы и самоуправления граждан. Например, инициативное бюджетирование в том числе на базе Единого портала государственных и муниципальных услуг (функций) (далее – «Госуслуги»), которое применяется в большей части субъектов Российской Федерации, позволяет активным гражданам непосредственно участвовать в финансировании проектов на своей территории. Проект Правительства Москвы «Активный гражданин» в рамках которого через сайт и мобильное приложение проводятся опросы жителей города, позволяет получить мнения горожан по актуальным вопросам, касающимся развития Москвы. Подобные цифровые платформы действуют в Санкт-Петербурге («Наш Санкт-Петербург»), в Московской области («Добродел»), Республике Татарстан («Народный контроль»), Нижегородской области («Нижегородская платформа электронной демократии»), Свердловской области («Екатеринбург. Решаем вместе!»), Красноярском крае («Жители Красноярского края»), Ханты-Мансийском автономном округе – Югра («Открытый регион –Югра»), Ямало-Ненецком автономном округе («Открытый Ямал») и других регионах России. Значительное распространение получили голосования на «Госуслугах». Например, в организованных Банком России обсуждениях обновления дизайна банкнот номиналом 500 рублей приняло участие более 1 млн человек в 2025 году; в народном голосовании за «Культурную столицу» – также более 1 млн человек в 2025 году. В выборах Президента Российской Федерации в 2024 году посредством дистанционного электронного голосования приняли участие 8 млн человек (из них на платформе «Госуслуги» участвовали почти 5 млн человек и на региональной московской платформе mos.ru еще 3 млн человек) [2].

Так реализуется российская модель «кибердемократии», которая представляет собой синтез традиционных демократических институтов и передовых телекоммуникационных технологий. Она подразумевает, что ответственный выбор гражданин будет делать значительно чаще чем раз в год на выборах государственных органов в единый день голосования. Для этого создаются различные «цифровые площадки» принятия решений: цифровые платформы в рамках развития умных городов, порталы государственных и

муниципальных услуг, общественного обсуждения проектов нормативных правовых актов. Однако пока цифровизация в основном затронула общественно-государственный диалог по вопросам местного значения и в значительно меньшей степени – проблемы общенационального масштаба и тем более вопросы оценки деятельности органов государственной власти.

Цифровая трансформация как основа новой системы легитимации власти. Российская Федерация провозглашает амбициозные цели в области цифровизации государственного управления и общественно-государственного диалога. В Указе Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» цифровая трансформация государственного и муниципального управления определена как ключевая цель национального развития (пп. «ж» ч. 1) [6]. Согласно пункту 8 Указа, целевой индикатор данной цели заключается в достижении к 2030 году «цифровой зрелости» государственного и муниципального управления, а также ключевых отраслей экономики и социальной сферы. Это предполагает автоматизацию значительной части транзакций в рамках единых отраслевых цифровых платформ. Также предусматривается переход к модели управления на основе данных, что включает ускоренное внедрение технологий обработки больших объемов данных и применение методов машинного обучения и искусственного интеллекта.

Основные изменения в системе ротации управленческих кадров предусмотрены в подпункте «з» пункта 8 Указа, который направлен на формирование комплексной системы подбора, развития и ротации специалистов для государственных органов и органов местного самоуправления. Данная система основывается на принципах равных возможностей, приоритета профессиональных компетенций и квалификаций, а также предусматривает внедрение механизмов регулярной оценки населением деятельности органов власти и обратной связи через единую цифровую платформу. Деятельность чиновников и органов власти должна регулярно оцениваться не только начальством, но и конечными «потребителями» их услуг – гражданами. К инструментам, позволяющим гражданам оценивать работу органов власти и конкретных государственных служащих, относятся: электронные анкеты и опросы, системы рейтингов на основе качества предоставления госуслуг, публикация результатов такой оценки, то есть создание элемента публичной конкуренции между регионами и ведомствами.

Представляется, что предусмотренный Указом Президента Российской Федерации «механизм регулярной оценки (управленческих кадров – прим. авт.) и обратной связи в рамках единой цифровой платформы» способен внести революционное изменение в традиционный механизм легитимации государственной власти. Он может быть включён в

него как составная часть, которая затронет как должностных лиц, избираемых населением в ходе голосования на выборах, так и назначаемых на должность, и будет реализовываться с широким участием граждан Российской Федерации.

Более того, при должном к нему подходе формируемый новый механизм легитимации государственной власти может стать основой для реализации принципа политической ответственности власти перед обществом и его внедрения в сферу реальной политики.

Включение механизмов обратной связи в систему легитимации власти. В мире известны два типа рекрутинга политических элит. Первый, –меритократический, – в России представлен традиционными конкурсами на замещение должностей государственной и муниципальной службы, неформальными практиками «протекции в продвижении по службе», а также новыми программами подготовки резерва управленческих кадров, такими как Высшая школа государственного управления РАНХиГС, конкурс «Лидеры России» и кадровая программа для участников СВО «Время героев». Второй, – демократический, – определяет формирование федеральных, региональных и муниципальных органов на основе демократических выборов.

Кроме того, исследователи избирательного права и процесса выделяют свободный мандат, согласно которому выборное должностное лицо не несёт прямой ответственности перед избирателями и императивный мандат, предполагающий возможность его отзыва. Последний после принятия в 2021 году Федерального закона «Об общих принципах организации публичной власти в субъектах Российской Федерации» распространяется в России только на членов выборных органов местного самоуправления [1, 7]. Таким образом возможности выразить своё доверие или недоверие избираемому должностному лицу у граждан ограничены избирательными процедурами.

Критерии оценки и интеграция с ключевыми показателями эффективности. Очевидно, что для «регулярной оценки и обратной связи в рамках единой цифровой платформы» необходимо установить ясные, универсальные и единые критерии такой оценки должностных лиц гражданами. Сегодня, например, для оценки деятельности глав субъектов Российской Федерации используются ключевые показатели эффективности (далее – КПЭ) – перечень экономических и социальных показателей, по которым Президентом Российской Федерации оценивается эффективность деятельности органов исполнительной власти субъекта Российской Федерации [5].

Начиная с 2024 года уже три из двадцати одного показателя: «Доверие к власти», «Удовлетворенность участников специальной военной операции условиями для медицинской реабилитации, переобучения и трудоустройства», «Удовлетворенность

граждан условиями для занятий физической культурой и спортом» формируются на основе мнения граждан. Остальные основываются на целевых статистических показателях и индикаторах, которые не предусматривают учёта мнения граждан [5].

Таким образом каждый из КПЭ высших должностных лиц субъектов Российской Федерации, избираемых в ходе периодических выборов, может иметь в дополнение к статистическому и социологический компонент, формирующийся на основе мнения (электронного опроса общественного мнения) избирателей. Например, существующий статистический КПЭ «Количество семей, улучшивших жилищные условия» может быть дополнен социологическим КПЭ «Удовлетворенность семей жилищными условиями» [5]. Представляется, что раскрытие в КПЭ губернаторов, наряду с данными экономической и социальной статистики по региону, зависимости выборного высшего должностного лица субъекта Российской Федерации от оценки его работы со стороны избирателей, способствовало бы повышению доверия к ним со стороны населения.

Для учёта мнения граждан может быть интересен опыт использования «Золотого стандарта», своеобразного чек-листа общественного контроля, с помощью которого граждане оценивают легитимность избирательного процесса. Нормативность и объективность критериев оценки, которые заложены в чек-листе общественного контроля в электоральной сфере, не отменяет субъективный характер и свободу принятия избирателем своего решения в ходе голосования [3]. Регулярная публичная оценка гражданами на основе установленных критериев деятельности должностных лиц, организованная на цифровой платформе, сделает периодические выборы более объективными и предсказуемыми.

Законодательная инициатива и перспективы развития.

В этой связи интересна законодательная инициатива, внесённая фракцией «Новые люди» в Государственную Думу в 2025 году [4]. В проекте федерального закона предлагается предоставить возможность гражданам ежегодно оценивать эффективность деятельности депутатов Государственной Думы, законодательного органа субъекта Российской Федерации, высшего должностного лица субъекта Российской Федерации, представительного органа муниципального образования, главы муниципального образования с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг» при тайном голосовании [5].

Указанная инициатива напрямую затрагивает вопросы осуществления общественного (гражданского) контроля в широком его понимании, поскольку направлена на формирование дополнительных механизмов обратной связи между обществом и органами публичной власти, а также на повышение уровня открытости и подотчётности

результатов деятельности соответствующих должностных лиц и представительных органов.

Несмотря на то, что внесенная парламентариями в Государственную Думу инициатива была ими позже отозвана для доработки, её ключевая идея представляется правильной и чрезвычайно актуальной.

Интеграция принципов общественной оценки в систему ключевых показателей эффективности деятельности высших должностных лиц субъектов Российской Федерации, а также реализация законодательной инициативы по ежегодной оценке деятельности высших должностных лиц регионов, депутатов и глав муниципальных образований могут существенно повысить уровень доверия граждан к власти и обеспечить более эффективный общественный контроль за деятельностью государственных и муниципальных органов.

Заключение. Внедрение механизмов регулярной оценки гражданами эффективности деятельности должностных лиц через единую цифровую платформу представляет собой перспективное направление развития демократических институтов в России. Этот механизм может стать важным шагом на пути преодоления общемирового кризиса представительной демократии, укрепления легитимности власти и обеспечения реальной обратной связи между обществом и государством.

Список источников и литературы:

1. Авакьян, С. А. Депутат: статус и деятельность / С. А. Авакьян // Конституционное и муниципальное право. –2021. –№ 7. –С. 3-11.
2. Заславский, С. Е. Система общественного контроля на российских выборах: развитие инфраструктуры и механизмы институционализации / С. Е. Заславский, Н. А. Тюков, В. А. Лукушин // Российский социально-гуманитарный журнал. – 2025. – № 2. – С. 102-103.
3. «Золотой стандарт» по общественному наблюдению за голосованием : утв. решением Совета Общественной палаты РФ от 27.02.2024 № 77-С [Электронный ресурс] // Общественная палата РФ. – URL: https://oprf.ru/structure_list/167 (дата обращения: 11.11.2025).
4. О внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс] : федер. законопроект № 1013051-8. – Режим доступа: https://sozd.duma.gov.ru/bill/1013051-8 (дата обращения: 11.11.2025).
5. Постановление Правительства Российской Федерации от 17.12.2021 г. № 2296 «Об утверждении перечня показателей для оценки эффективности деятельности высших должностных лиц (руководителей высших исполнительных органов государственной власти) субъектов Российской Федерации и деятельности органов исполнительной власти субъектов Российской Федерации» [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202112170044 (дата обращения: 11.11.2025).
6. Указ Президента Российской Федерации от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [Электронный ресурс] // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202007210012 (дата обращения: 25.10.2024).
7. Федеральный закон от 21.12.2021 №414-ФЗ «Об общих принципах организации публичной власти в субъектах Российской Федерации»
8. Шмиттер Ф. К. Будущее демократии: можно ли рассматривать его как нелинейный процесс? // Полис. Политические исследования. 2022. № 2. С. 8-29.
9. Politico: несколько западных демократий столкнулись с кризисом доверия к власти // ТАСС. – 2024. –25 сент. – URL: https://tass.ru/mezhdunarodnaya-panorama/19506471 (дата обращения: 11.11.2025).
10. What can be done to arrest the trend of democratic decline worldwide? : In Focus podcast // The Hindu. – 2024. –28 August. – URL: https://www.thehindu.com/podcast/what-can-be-done-to-arrest-the-trend-of-democratic-decline-worldwide-in-focus-podcast/article68663648.ece (дата обращения: 11.11.2025).

Тигран Давидович Оганесян,
к.ю.н., доцент кафедры международного права
Дипломатической академии МИД России
E-mail: t.oganesian@mail.ru

Tigran D. Oganesian,
Candidate of Law, Associate Professor of the Department of International Law
The Diplomatic Academy of the Russian Ministry of Foreign Affairs
E-mail: t.oganesian@mail.ru

СОВРЕМЕННЫЕ ВЫЗОВЫ ЗАЩИТЫ ДАННЫХ В УСЛОВИЯХ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

MODERN CHALLENGES OF DATA PROTECTION IN THE CONTEXT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

Аннотация. Эффективность некоторых традиционных подходов, гарантирующих защиту данных, в настоящее время существенно снижается и происходит поиск новых подходов, которые бы смогли отвечать реалиям сегодняшнего дня. В этой связи вопросы защиты персональных данных приобретают еще большее значение в контексте развития и массового внедрения программ и методов автоматизированной обработки данных. Возникает также особая необходимость в переосмыслении природы права на защиту данных и выработки новых стандартов международной защиты от соответствующих злоупотреблений в связи с использованием новых информационно-коммуникационных технологий.

Ключевые слова: защита персональных данных; искусственный интеллект; право на уважение частной жизни; Интернет.

Abstract. The effectiveness of some traditional approaches guaranteeing data protection is currently significantly decreasing and new approaches are being sought that could meet the realities of today. In this regard, the issues of personal data protection are becoming even more important in the context of the development and mass implementation of automated data processing programs and methods. There is also a particular need to rethink the nature of the right to data protection and to develop new standards for international protection against related abuses in connection with the use of new information and communication technologies.

Keywords: personal data protection; artificial intelligence; right to respect for privacy; Internet.

За последние десятилетия технические возможности для сбора и обработки данных существенно расширились. Цифровая революция и технологический прогресс не только изменили отношение людей к персональным данным, но и, в свою очередь, бросили вызов существующим концепциям и средствам правовой защиты данных. В настоящее время мы ежедневно «загружаем» в глобальную сеть огромное количество персональных данных. Это происходит чаще всего в социальных сетях, когда, к примеру, мы публикуем информацию, загружаем фотографии или видео, играем в онлайн-игры: эти действия непосредственным образом генерируют наши данные. Мы также создаем персональные данные в автономном режиме, когда совершаем телефонные звонки, оплачиваем покупки банковской картой или пользуемся общественным транспортом.

Вопросы защиты персональных данных приобретают еще большее значение в контексте развития и массового внедрения программ и методов автоматизированной обработки данных. Телекоммуникационные компании ежегодно предоставляют большое количество данных правительственным службам в ответ на требования властей [3, p. 104]. В этой связи сложно не согласиться с С. Честерманом, что «усилия по защите частной жизни вынуждены реагировать на новые угрозы и технологии» [4, p. 414].

Большие данные (Big Data) собираются крупными корпорациями и правительствами, которые анализируют их с помощью различных компьютерных программ и алгоритмов. Компьютеры, мобильные устройства и различные смарт-устройства значительно расширили возможности хранения и обработки данных в больших масштабах. Проблема защиты данных осложняется также расширяющимся кругом субъектов, занимающихся сбором и обработкой данных. Современный французский философ Б. Стиглер справедливо описывает произошедший сдвиг, основанный на развитии смарт-устройств, в сторону «общества гиперконтроля» [9, p. 76]. Произвольный сбор данных в некоторых случаях представляет угрозу не только праву на уважение частной жизни, но и приводит к другим нарушениям. Например, как отметил Комитет министров Совета Европы массовый сбор данных способствует «сортировке людей по категориям, тем самым усиливая различные формы социальной, культурной, религиозной, правовой и экономической сегрегации и дискриминации» [1].

В этой связи в эпоху «Big Data» эффективность некоторых традиционных подходов, гарантирующих защиту от произвольного использования данных, существенно снижается и происходит поиск новых подходов, которые бы смогли отвечать реалиям сегодняшнего дня. Если несколько лет назад европейская нормативная база в области защиты персональных данных была весьма фрагментарным и не существовало правового единообразия, то сегодня Совет Европы и Европейский Союз приняли соответствующие

документы, призванные восполнить пробелы и гарантировать юридическое единообразие между государствами в вопросах защиты данных. Определенную роль в развитии права на защиту данных в прецедентной практике выполняют Европейский Суд по правам человека (далее – ЕСПЧ) и Суд Европейского Союза (далее – Суд ЕС), позиции которых по вопросу «автономности» и самостоятельности права на защиту данных от права на уважение частной жизни отличаются друг от друга. Существующая связь между правом на уважение частной жизни и защитой персональных данных обусловленная эволюцией европейской системы защиты персональных данных, неоднозначно расценивается не только отдельными исследователями, но и не перестала признаваться отдельными государствами-членами Европейского Союза. В этой связи представляется целесообразным рассмотрение в рамках настоящей статьи в том числе подходов современных ученых к решению данного вопроса, а также актуальной прецедентной практики ЕСПЧ и Суда ЕС, чьи правовые позиции играют доминирующую роль в Европе в определении векторов развития права на защиту данных.

Принятие первых национальных законов о защите данных было обусловлено возникшей компьютеризацией, поэтому большинство национальных законов ограничивалось лишь автоматизированной обработкой данных. В 1970-х гг. в нескольких европейских странах (ФРГ, Швеция и Франция) стали появляться различные положения, регулирующие автоматизированную обработку данных. Принимаемые законы устанавливали собственные подходы защиты физических лиц в отношении автоматизированной обработки данных, применяя различную терминологию. В качестве символической отправной точки защиты данных на национальном уровне в Европе определяется принятие в 1970 г. германской федеральной землей Гессен первого закона о защите данных (*Datenschutz)*. Последовав данному примеру, спустя пару лет Швеция в 1973 г. также приняла подобный закон *Datalag,* а в 1978 г. французский парламент одобрил закон *informatique et libertés* (компьютеры и свободы). Важным аспектом изучения является то, что принятые положения не связывали право на защиту данных с каким-либо иным основополагающим правом. Например, шведский закон 1973 г., регулирующий автоматизированную обработку данных, не увязывал защиту данных с правом на уважение частной жизни и конфиденциальностью. Заявленная цель шведского акта заключалась в защите неприкосновенности личности. Французский закон *Loi informatique et liberté* [7], в свою очередь, был нацелен на защиту vie privée (частной жизни) и связывал защиты данных с правом на уважение частной жизни. Аналогичным образом австрийские конституционные положения о защите персональных данных 1978 г., закрепив впервые право на защиту

данных (*datenschutz*) в качестве конституционного права, связывали защиту данных с правом на уважение частной и семейной жизни [5].

Таким образом, в большинстве случаев, когда государства решались на закрепление положений об обработке данных, это осуществлялось в форме отдельных законов (например, во Франции), однако в некоторых случаях положения об автоматизированной обработке данных находили свое отражение в принятых конституциях (например, в Португалии, Испании). Можно также заметить, что в 1970-е гг. принятые акты касались прежде всего автоматизированной обработки данных и содержали именно данную формулировку. Подобные законы о защите данных, принятые в Европе на национальных уровнях в 1970-е гг., характеризовались расплывчатостью формулировок относительно преследуемых целей или задач. Однако в конечном счете все эти нормы и правила заложили основу для развития национальных законодательств в сфере защиты данных, а также для создания средств правовой защиты. Позже разработанные положения и практика в области защиты данных вышеперечисленных государств послужат основой для разработки Конвенции 108 и Директивы ЕС 1995 г.

1990-е стали эпохой широкого распространения персональных компьютеров и Интернета. Впервые в мире Тимом Бернерс-Ли был создан и запущен веб-сайт (1991), была спроектирована культовая операционная система Windows 95 с кнопкой «Пуск» (1995), разработан язык программирования Java (1995). Идея признания права на защиту данных для противодействия угрозам технологического прогресса на уровне ЕС впервые появилась в докладах экспертов в контексте Амстердамского договора в конце 1990-х гг. [10]

Профессор Брюссельского университета Г. Гонсалес Фустер справедливо отмечает, что к этому времени «защита данных» означала защиту данных, подвергающихся лишь автоматизированной обработке, указывая на то, что данная дефиниция была заимствована из немецкого слова «*Datenschutz»* [6, p. 86]. Данное значение, по наблюдению Г. Гонсалес Фустер, было утрачено в последующем при переводе транснациональных документов о защите данных, и перечень данных был существенно расширен.

Заключение. Проведенный анализ эволюции национальных и общеевропейских норм о защите данных свидетельствует о том, что длительное время оно рассматривалось юристами, политиками и учеными как «маргинальное и техническое» [8, p. 253]. Тем не менее, такое восприятие быстро исчезло, поскольку защита данных оказалась в центре внимания по ряду причин. Во-первых, резкое увеличение масштабов обработки персональных данных неизбежно привело к необходимости установления единых стандартов и норм сбора и обработки данных. Во-вторых, право на защиту данных было признано на международном уровне в прецедентных практиках Суда ЕС и ЕСПЧ [2].

Безусловно, развитие искусственного интеллекта (ИИ) создает принципиально новые вызовы для защиты персональных данных и приватности. Эти вызовы носят системный характер и затрагивают правовые, технологические и этические аспекты. Классические принципы, закрепленные в таких нормах, как GDPR (Общий регламент по защите данных в ЕС), оказываются под давлением.

Цель обработки и минимизация данных: ИИ, особенно модели машинного обучения, часто требуют огромных объемов данных («большие данные») для обучения. Заранее бывает сложно или невозможно определить все возможные цели и законные основания для их использования. Принцип «собирай только необходимое» вступает в противоречие с логикой ИИ «чем больше данных, тем точнее модель».

Прозрачность и объяснимость («Право на объяснение»): Многие сложные модели ИИ, особенно глубокое обучение, работают как "черные ящики". Даже их создатели не всегда могут точно объяснить, почему модель приняла то или иное конкретное решение (например, отказала в кредите или отфильтровала резюме). Это делает практически невозможным выполнение требований о предоставлении субъекту данных понятной информации о логике автоматизированной обработки.

Точность и актуальность данных: ИИ может делать выводы и прогнозы о человеке на основе косвенных или обезличенных данных. Эти прогнозы (например, о вероятности совершения преступления, кредитоспособности, состоянии здоровья) могут быть неточными или дискриминационными, но при этом оказывать реальное влияние на жизнь человека. Как регулировать точность не исходных данных, а выводов, сделанных алгоритмом?

Развитие ИИ не просто создает новые угрозы утечек данных; оно подрывает сами основы традиционной системы защиты данных, построенной на принципах согласия, целеполагания и прозрачности. Современные вызовы требуют перехода от реактивной защиты к проактивному управлению рисками, глубокой интеграции юридических и технологических подходов и глобального диалога о том, как совместить технологический прогресс с фундаментальными правами человека.

Список источников и литературы:

1. Декларация Комитета министров Совета Европы о манипулятивных возможностях алгоритмических процессов. Decl(13/02/2019)1. (Принята 13 февраля 2019 г. на 1337-ᴹ заседании). URL: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b (дата обращения: 12.09.2025).

2. Постановления Суда ЕС по делам: Volker und Markus Schecke and Hartmut Eifert, Joined Cases C-92/09 and C-93/09, EU: C:2010:662. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, EU: C:2014:238.

3. Brown I. Communications Data Retention in an Evolving Internet // International Journal of Law and Information Technology. 2011. Vol. 19. Issue 2. Pp. 95–109.

4. Chesterman S. After Privacy: The Rise of Facebook[2], the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012 // Singapore Journal of Legal Studies. 2012. Pp. 391–415.

5. Data Protection Act, BGBl. No. 565/1978.

6. Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing. 2014. 274 p.

7. Loi № 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig (дата обращения: 12.09.2025).

8. Lynskey O. The «Europeanisation» of Data Protection Law // Cambridge Yearbook of European Legal Studies. 2017. Vol. 19. Pp. 252–286.

9. Stiegler B. La Société automatique: L'avenir du travail, Paris: Fayard. 2015. 280 p.

10. Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts [1997] OJ C340/1 (Treaty of Amsterdam).

[2] Принадлежит компании Meta, признанной экстремистской и запрещённой на территории РФ.

Наталья Валерьевна Савельева,
научный сотрудник
Институт физики Земли им. О.Ю. Шмидта РАН,
выпускник магистратуры МГЮА им. О.Е. Кутафина,
независимый исследователь в области
международного космического права
E-mail: nasa2000@yandex.ru

Natalie V. Savelyeva
Researcher at Schmidt Institute of the Earth Physics
of the Russian academy of science
Magister of International Law, Kutafin Moscow State Law University,
Independent Researcher in the International Space Law
E-mail: nasa2000@yandex.ru

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ В КОСМОСЕ

INTERNATIONAL LEGAL REGULATION OF SPACE DATACENTERS

Аннотация. Рассматриваются проблемы международно-правового регулирования деятельности по созданию и эксплуатации центров обработки данных на орбитах вокруг земли, с учетом специфики физического и виртуального сегментов, приводится обзор существующих международно-правовых инструментов в области кибер-безопасности подобных систем.

Abstract. The problems of international legal regulation of activities related to creation and operation of future space data centers are considered. Special attention is given to the issues of liability for illegal actions against, or by means of such data centers.

Ключевые слова: международное космическое право, информационно-коммуникационные технологии, информационная безопасность, кибер-преступления, космические центры обработки данных.

Key words: international space law, information and communication technologies, information security, space datacenters.

Введение. Центры обработки данных (ЦОД) необходимы для поддержки работы и развития систем искусственного интеллекта (ИИ) и технологий на их основе. Для поддержания работы ЦОД необходимо много электроэнергии и других ресурсов. Аналитики оценивают рост в потреблении энергии со стороны ИИ на базе ЦОД в 165% относительно современного общего уровня потребления всеми ЦОД к 2030 году [10]. В космосе нет проблем с получением энергии от солнечных батарей, охлаждением,

поддержкой стабильного микроклимата внутри ЦОД, а магнитное поле Земли защищает систему от ионизирующих космических излучений и солнечного ветра (если спутник находится на низкой или средней орбите, которая не пересекает радиационные пояса Земли). По прогнозам, в ближайшие годы в космос будут выведены десятки ЦОД мощностью в десятки и сотни гигаватт. Уже реализованы несколько пилотных проектов в области создания дата-центров и серверных мощностей на орбите. К примеру, российский спутник-сервер RUVDS [3], запущенный в 2023 году, а также RUVDSSat1 [5], который планировали запустить в 2025 году. Также существует ряд проектов создания полноценных ЦОД в космосе, к примеру, полностью частный проект Starcloud [12], который реализуется [15] с участием таких гигантов, как Google и NVIDIA. Компания Starlink также планирует начать строительство ЦОД на орбите на базе спутников Starlink поколения V3 [14].

Технических сложностей и рисков при создании и эксплуатации ЦОД много, включая проблемы обмена данными, ремонта, обновления оборудования, но все они решаемы. Вопрос в том, что делать с юридическими аспектами переноса в космос огромных массивов данных и средств их обработки и хранения? Как разрешать спорные вопросы в случае несанкционированного доступа к данным, либо вмешательства в работу оборудования, учитывая особенности особый правовой статус космического пространства?

Космос и кибер-пространство имеют одну схожую черту: сложность в демаркации границ. Особый правовой статус космического пространства и небесных тел, закрепленный в Договоре по космосу 1967 года [1] и других основополагающих документах международного космического права (МКП), о сути своей, делает невозможным расширение границ государств за счет национализации космоса или небесных тел. Юрисдикция государства в полной мере распространяется на пространство внутри космических аппаратов, внесенных в реестр на имя такого государства. Таким образом, в космосе физической основой юрисдикции государства остаются космические аппараты, станции, иные конструкции, искусственные сооружения, зарегистрированные от имени государства.

Физической основой кибер-пространства являются информационно-коммуникационные системы (ИКС), включая распределенные, когда отдельные сегменты системы разнесены по разным странам, континентам, а в недалеком будущем и планетам. В отличие от космических аппаратов, физическая часть ИКС не является объектом экстерриториальной юрисдикции. С виртуальным сегментом (информация, виртуальное пространство, созданное на базе ИКС) дела обстоят сложнее. К примеру, Генеральный регламент по защите персональных данных ЕС [4] допускает экстерриториальное

применение, если речь идет о персональных данных граждан (подданных) стран-участник ЕС.

Таким образом, при использовании ЦОД в космосе следует разграничивать физический и виртуальный слои. Оборудование ЦОД является частью космического аппарата, следовательно, находится в юрисдикции государства регистрации такого аппарата. Деятельность по созданию и эксплуатации ЦОД может осуществляется любыми лицами, органами власти, транснациональными корпорациями (к примеру, Google, Amazon), юридическими лицами по национальному праву, даже физическими лицами. Т.е. владельцем оборудования ЦОД может быть кто угодно, от физлица до суверенного государства. То же касается хранящихся в ЦОД данных. К примеру, Google или любая другая компания может использовать ЦОД в качестве «облака» для хранения данных пользователей своих сервисов. В физическом пространстве локализовать виртуальный сегмент ЦОД крайне сложно, как и отделить его от наземного.

Вопрос защиты данных, трансграничного доступа к данным, разграничения полномочий при разрешении споров и расследовании различного рода инцидентов, включая вопросы уголовной юстиции, касается обоих сегментов, так как для работы с данными необходимы оба компонента: носители для хранения и виртуальная среда для работы с данными.

Вопросы кибер-безопасности в настоящее время регулируются целым рядом международно-правовых документов. В Конвенции о преступности в сфере компьютерной информации ETS 185, подписанной 23 ноября 2001 года в Будапеште [16], предусмотрены четыре состава преступлений с использованием ИКТ, включая незаконный доступ к данным и информационным системам, нарушение их целостности и т.д. Также имеется ряд соглашений, направленных введение соответствующих положений в национальное законодательство, а также унификаций национальных законов разных стран. К примеру, участники СНГ подписали Соглашение о сотрудничестве в борьбе с преступлениями в сфере информационных технологий [7], что позволило стандартизировать составы преступлений и согласовать процедуры взаимодействия при расследовании. Участники Лиги арабских государств подписали Конвенцию о борьбе с преступлениями в области информационных технологий 2010 года [11] с целью унификацию национального законодательства. Соглашение о сотрудничестве в области обеспечения международной информационной безопасности 2010 года [6] подписано странами ШОС с целью совместной защиты от кибер-угроз. Аналогичной цели служит и Конвенция Африканского союза о кибер-безопасности и защите персональных данных 2017 года [9]. Директива ЕС об атаках на информационные системы [13] принята с целью унификации национального

законодательства стран-участников ЕС путем введения уголовной ответственности за масштабные кибер-атаки на объекты инфраструктуры. Общий/Генеральный регламент по защите персональных данных ЕС [4], который представляет собой ряд директив ЕС, был введен во всех странах ЕС в 2018 году и до сего дня является основным законом, регулирующим вопросы защиты персональных данных на территории ЕС, с учетом экстерриториальности применения его положений при ряде условий.

В 2024 году резолюцией ГА ООН одобрен текст Всеобъемлющей конвенции по кибер-преступности [2, 8] (далее – «Конвенция»), которая модельный закон по борьбе с кибер-преступностью, включая описание составов кибер-преступлений, процессуальные полномочия и ограничения при расследовании оных, процедуры взаимодействия уполномоченных органов. Конвенция предусматривает уголовную, административную, гражданско-правовую ответственность для физических и юридических лиц. Следует отметить особую роль представителей Российской Федерации в создании и принятии Конвенции.

Заключение. Вывод ЦОД в космос только начинается, потому реальная судебная практика разрешения связанных с ЦОД трансграничных споров отсутствует. Тем не менее, основы нормативной базы заложены, работа по созданию орбитальных ЦОД уже ведется. Не за горами первые дела, первые споры, связанные с созданием и эксплуатацией ЦОД.

Список источников и литературы:

1. Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела. Принят резолюцией 2222 (XXI) Генеральной Ассамблеи от 19 декабря 1966 года. Официальный сайт ООН. [URL: https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml (дата обращения: 05.11.2025).

2. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям. Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243?ysclid=mhw0gembr4620271919 (дата обращения: 05.11.2025)

3. Космический ЦОД. URL: https://sputnik.rucloud.host/ (дата обращения: 05.11.2025)

4. Общий/Генеральный регламент по защите персональных данных. Регламент (EU) 2016/679. Директива (EU) 2016/680. URL: https://ogdpr.eu/ru/gdpr-2016-679 (дата обращения: 05.11.2025)

5. RUVDS приступили к испытаниям спутника-платформы https://ruvds.com/ru/ruvds_ruvdssat1_final_countdown/ (дата обращения: 05.11.2025)

6. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=198&nd=203002652&collection=1&ysclid=m2k8o7u5p4639107584 (дата обращения: 05.11.2025)

7. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, Душанбе, 28 сентября 2018 года. Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005?ysclid=m2g7a621x9793411749 (дата обращения: 05.11.2025)

8. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (Accessed: 05.11.2025).

9. African Union Convention on Cyber Security and Personal Data Protection. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (Accessed: 05.11.2025)

10. AI to drive 165% increase in data center power demand by 2030. URL: https://www.goldmansachs.com/insights/articles/ai-to-drive-165-increase-in-data-center-power-demand-by-2030 (Accessed: 05.11.2025)

11. Arab Convention on Combating Information Technology Offences. URL: https://itlaw.fandom.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences (Accessed: 05.11.2025)

12. Data centers in Space. Starcloud. Official site. URL: https://www.starcloud.com/ (дата обращения: 05.11.2025)

13. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF (Accessed: 05.11.2025)

14. Elon Musk on data centers in orbit. ArsTechnica, 31.10.2025. URL: https://arstechnica.com/space/2025/10/elon-musk-on-data-centers-in-orbit-spacex-will-be-doing-this/ (Accessed: 05.11.2025).

15. Starcloud-1 satellite reaches space, with Nvidia H100 GPU now operating in orbit. Data Centre Dynamics. 03.11.2025. URL: https://www.datacenterdynamics.com/en/news/starcloud-1-satellite-reaches-space-with-nvidia-h100-gpu-now-operating-in-orbit/ (Accessed: 05.11.2025)

16. The Budapest Convention (ETS No. 185) and its Protocols. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 22.10.2024).

Алиса Михайловна Слесарева,
Студент ФГБОУ ВО «КНИТУ»
Казань, Россия
Научный руководитель: Шевко Наиля Рашидовна,
кандидат экономических наук,
доцент кафедры «Информационная безопасность»
E-mail: slesarevaalisa03@gmail.com

Alisa M. Slesareva,
Student of the Federal State Educational Institution
of Higher Education "KNRTU"
Kazan, Russia
Supervisor: Nailya Rashidovna Shevko,
PhD in Economics, Associate Professor of the
Department of Information Security
E-mail: slesarevaalisa03@gmail.com

ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

LEGAL PROTECTION OF INFORMATION IN SOCIAL NETWORKS

Аннотация. В данной статье рассматривается правовая защита информации в социальных сетях как актуальная проблема современного цифрового общества. Анализируется роль социальных сетей в коммуникации, распространении информации, организации досуга и профессиональной деятельности, а также выявляются основные риски, связанные с незаконным использованием данных пользователей. Особое внимание уделяется существующей нормативной базе, практике применения уголовного и административного законодательства, а также выявленным пробелам в правовом регулировании. Предлагаются меры по совершенствованию законодательства и повышению эффективности защиты информации в цифровой среде.

Ключевые слова: информационное общество, цифровые технологии, право, защита информации, социальные сети.

Abstract: This article examines the legal protection of information on social media as a pressing issue in today's digital society. It analyzes the role of social media in communication, information dissemination, leisure, and professional activities, and identifies the key risks associated with the illegal use of user data. Particular attention is paid to the existing regulatory framework, the application of criminal and administrative law, and identified gaps in legal regulation. Measures are proposed to improve legislation and enhance the effectiveness of information protection in the digital environment.

Key words: information society, digital technologies, law, information protection, social network.

Под правовой защитой информации в социальных сетях следует понимать систему правовых норм, направленных на регулирование отношений, возникающих при сборе, обработке, хранении и распространении данных пользователей. Она включает в себя нормы конституционного, административного, уголовного и информационного права. Ключевыми задачами правовой защиты выступают обеспечение конфиденциальности, предотвращение неправомерного доступа, защита от распространения противоправного контента, а также охрана чести, достоинства и деловой репутации граждан. [3; 7]

Актуальность исследования. Социальные сети сегодня являются неотъемлемым элементом общественной жизни, применяются как в личных, так и в профессиональных целях, включая деловую и политическую активность. Вместе с тем эти платформы нередко используются для совершения противоправных действий. Распространение экстремистских материалов, мошенничество, кибербуллинг и незаконная обработка персональных данных подчёркивают актуальность исследования в этой области [5; 8].

Статистические данные. Согласно сведениям МВД России, более 70 % преступлений, связанных с мошенничеством в 2022 году, совершались с использованием интернет-ресурсов, включая социальные сети [4]. В том же году Роскомнадзор ограничил доступ к более чем 120 000 сайтов, содержащих запрещённую информацию [6]. Опросы ВЦИОМ показывают, что около 63 % граждан сталкивались с попытками обмана в социальных сетях, что подтверждает массовый характер угроз [1].

Практика применения законодательства. Уголовно-правовая практика [5]:

− статья 128.1 УК РФ («Клевета») применяется к случаям распространения ложных сведений, наносящих ущерб чести и достоинству граждан в соцсетях;

− статья 280 УК РФ («Публичные призывы к осуществлению экстремистской деятельности») предусматривает уголовную ответственность за публикацию материалов экстремистского характера;

− статья 282 УК РФ («Возбуждение ненависти либо вражды») направлена против лиц, распространяющих контент, разжигающий вражду на национальной, расовой или религиозной почве.

Практика показывает, что значительная часть дел связана с использованием социальных сетей для распространения экстремистских идей и координации противоправной деятельности, в том числе в исправительных учреждениях. В ФСИН

фиксируются случаи, когда заключённые использовали соцсети для связи с сообщниками или распространения запрещённой информации.

Административно-правовая практика [2]:

– статья 20.3.1 КоАП РФ («Возбуждение ненависти либо вражды, унижение человеческого достоинства») применяется к менее тяжким правонарушениям;

– статья 13.15 КоАП РФ («Злоупотребление свободой массовой информации») используется для пресечения публикаций заведомо недостоверной информации.

Таким образом, практика показывает комплексный подход к защите информации: от уголовной ответственности за серьёзные нарушения до административных мер за менее опасные деяния.

Проблемные аспекты законодательства. Несмотря на наличие нормативной базы, законодательно не урегулированы некоторые ключевые вопросы [7]:

– не полностью определена ответственность социальных сетей за контент пользователей;

– отсутствуют механизмы противодействия трансграничным угрозам со стороны иностранных платформ;

– недостаточна защита жертв кибербуллинга и интернет-сталкинга;

– ограничены возможности расследования преступлений, совершённых с использованием технологий анонимизации (VPN, TOR).

Предложения по совершенствованию законодательства.

– закрепить обязательства социальных сетей по выявлению и блокировке противоправного контента;

– разработать международные соглашения, направленные на противодействие киберпреступлениям и регулирование деятельности транснациональных платформ;

– расширить программы правового просвещения в области информационной безопасности среди населения, включая подростков и молодежь.

Заключение. Защита информации в социальных сетях является важным элементом обеспечения безопасности граждан и общества. Несмотря на существующую нормативную базу, сохраняются пробелы, требующие совершенствования законодательства. Усиление ответственности платформ, международное сотрудничество и внедрение дополнительных механизмов защиты способны повысить эффективность правовой защиты пользователей цифрового пространства.

Список источников и литературы:

1. Всероссийский центр изучения общественного мнения. Социальные сети и интернет-безопасность: результаты всероссийского опроса (2022): [Электронный ресурс]. – URL: [https://wciom.ru] (Дата обращения: 6.11.2025).

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (в последней редакции) : Закон. – М., 2023.

3. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г., с учётом поправок 2020 г. – М., 2020.

4. Министерство внутренних дел Российской Федерации. Отчёт о состоянии преступности в 2022 году: [Электронный ресурс]. – URL: [https://mvdmedia.ru] (Дата обращения: 6.11.2025).

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в последней редакции): Закон. – М., 2023.

6. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Отчёт за 2022 год: [Электронный ресурс]. – URL: [https://rkn.gov.ru] (Дата обращения: 6.11.2025).

7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: Закон. – М., 2006.

8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: Закон. – М., 2006.

Алёна Дмитриевна Цыплакова,
Преподаватель кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД России, соискатель учёной степени к.ю.н.,
студент 1 курса магистратуры «Искусственный интеллект» МГИМО МИД России (Одинцовский филиал) совместно с МФТИ,
E-mail: tsyplakova.a.d@my.mgimo.ru

Alyona D. Tsyplakova,
Lecturer of the Department of Criminal Law, Criminal Procedure and Criminology of MGIMO University, PhD candidate,
Master's Degree student of AI program (MGIMO-Odinstovo, MPIT)
E-mail: tsyplakova.a.d@my.mgimo.ru

КОНВЕНЦИЯ ООН ПРОТИВ КИБЕРПРЕСТУПНОСТИ: НОВШЕСТВА, ПЕРСПЕКТИВЫ И ТРУДНОСТИ ИМПЛЕМЕНТАЦИИ ДЛЯ ОТДЕЛЬНЫХ СТРАН ГЛОБАЛЬНОГО ЮГА

UN CONVENTION AGAINST CYBERCRIME: NOVATIONS, OUTLOOK AND IMPLEMENTATION ISSUES FOR CERTAIN GLOBAL SOUTH COUNTRIES

Аннотация. Автором представлен краткий обзор новшеств открытой к подписанию Ханойской конвенции против киберпреступности, возможные трудности, с которыми столкнутся государства Глобального Юга при имплементации её положений, а также перспективы развития положений данного документа и содержания вероятных дополнительных протоколов.

Ключевые слова: противодействие преступлениям, киберпреступления, ООН, Глобальный Юг.

Abstract. The author presents a brief overview of the innovations of the Hanoi Convention against Cybercrime, which has been now open for signing, possible difficulties that the Global South states are likely to face in implementing its provisions, as well as the prospects for the document development and the content of the possible additional protocols.

Key words: crime prevention, cybercrimes, the United Nations, Global South.

Несмотря на то, что внесённый Российской Федерации проект Конвенции претерпел ряд изменений (в особенности в части составов преступлений и международного правоохранительного содействия) в сравнении с Конвенцией ООН против киберпреступности; укрепление международного сотрудничества в борьбе с

определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям [3], отметим следующие достоинства итогового документа:

– единообразие терминологии, разработанной на основании консолидированной позиции группы по языковому соответствию, где были представлены страны Глобального Севера и Глобального Юга (при полном или хотя бы частичном совпадении позиций КНР, Индии, Индонезии, РФ, ИРИ, АРЕ и АНДР);

– соблюдение прав человека как отдельное направление;

– универсальный механизм для целей международного сотрудничества в сфере уголовного судопроизводства (МССУС) без условностей, но только по перечисленным серьёзным преступлениям;

– применимость положений Конвенции к стадиям предотвращения преступлений, в том числе выявления и пресечения;

– сеть 24/7.

При этом они же одновременно могут расцениваться и как препятствия при имплементации. Например, в то время как согласно Рекомендациям ФАТФ [11] и Руководству по применению риск-ориентированного подхода в отношении виртуальных активов и провайдеров виртуальных услуг [12] виртуальные активы являются устойчивым термином (и для целей Конвенции признаются имуществом), в России понятийно-категориальный аппарат и правовые статусы отдельных объектов отличаются. В ряде государств (e.g., Индия, Индонезия и Иран) невозможна конфискация имущества без обвинительного приговора.

Страны Глобального Юга делали довольно прогрессивные предложения в части юрисдикционных привязок: дополнение космическими объектами / спутниками, принадлежность домена Интернет-ресурса, принадлежность данных, места расположения серверов онлайн-сервисов, используемых для осуществления преступной деятельности, местоположение поставщиков сетевых услуг, местонахождение нарушенных информационных сетевых систем и их менеджеров, а равно информационных систем, которые использовались подозреваемыми, обвиняемыми или потерпевшими, места, где потерпевшим нанесен вред или где имели место потери имущества [13], однако все они так или иначе были отвергнуты [6]. Проблема демаркации киберпространства всё чаще и острее стоит на повестке, однако всё ещё пока не разрешена [14].

С точки зрения доказательств в электронной форме отметим неготовность отечественного законодательства с точки зрения правового статуса и используемых

следственных действий для закрепления доказательственной информации (в отличие от остальных стран-участниц СНГ [10]). Также отсутствуют уже традиционные для универсальных конвенций негласные специальные методы расследования. При условии требований к передаче данных поставщиками услуг отметим отсутствие единообразных сроков хранения данных (в странах Глобального Юга варьируются от 15 дней до нескольких лет), понятия незаконного контента и процедур блокировки (административной, судебной или смешанной) [11].

При условии разработки реестра (дипломатических и технических) контактных пунктов, а также сети 24/7 проводимые пинг-тесты и проверки показывают скорее формальный подход многих государств, нежели действительное желание сотрудничать [16].

	Количество контактных пунктов в реестре	Количеств ответивших контактных пунктов	Доля ответивших контактных пунктов	Количество стран, участвующих в реестре	Страны, у которых не ответил ни один контактный пункт	Доля не ответивших стран
Первый пинг-тест с уведомлением (июнь 2024)	243	176	72%	99	12	12%
Второй пинг-тест с уведомлением (декабрь 2024)	281	179	64%	112	20	18%
Первый пинг-тест без уведомления (июнь 2025)	307	177	58%	115[3]	24	21%

Таблица № 1. Данные о контактных пунктах и их реакции на пинг-тесты

В дополнение стоило бы реализовать банки (учёты) электронных / цифровых следов для снижения нагрузки и избежания повторных запросов по схожим обстоятельствам [1, 2], лицам или идентификационным данным, а также защищённые платформы / каналы связи

[3] Примерная цифра. На октябрь 2025 г. присоединилась 121 государство.

для полноценного взаимодействия по линии МССУС и международного полицейского сотрудничества и имплементации электронного документооборота [7].

Неохваченным остаются и новые вызовы и угрозы, к которым можно отнести мета-вселенные, технологии искусственного интеллекта (в первую очередь генеративные или большие языковые модели), электронные мухи [18] и цифровые наркотики [19]. Наконец, применимость норм МГП в киберпространстве также не охвачена, хотя может и стать предметом Дополнительного протокола, исходя из позиции Омана [17].

На данный момент[4] подписантами являются 72 государства, только одно из которых сделало оговорки (Азербайджан), хотя, как показывает практика ратификации так называемых Меридской и Палермской конвенций [4, 5], не исключено, что возможности использования традиционных механизмов МССУС будут ограничены: например, Конвенция ООН против коррупции (Мерида, 31.10.2003) не является правовым основанием для выдачи, например, по оговоркам КСА, Кубы и Сальвадора, в отсутствие двустороннего международного договора [8], Конвенция ООН против транснациональной организованной преступности (Палермо, 15.11.2000) – например, для Вьетнама [9]. Однако среди подписантов Ханойской конвенции нет в целом стратегических партнёров Российской Федерации и иных крупных игроков (технологических держав), в том числе США, Республики Индия, ОАЭ, Кувейта, Иорданского Хашимитского Королевства, Королевства Бахрейн, Султаната Омана, Таджикистана, Туркменистана, Кыргызстана, ФРГ, Италии, Швейцарии, Северной Европы, Республики Корея, Государства Япония, Сингапура, что также может сказаться на межгосударственном взаимодействии, поскольку ряд провайдеров услуг, мессенджеров, социальных сетей, а равно оборудование для обеспечения работы генеративных моделей ИИ расположены в недружественных юрисдикциях.

Заключение. Таким образом, несмотря на дипломатическую победу России в контексте противодействия киберпреступлениям на межгосударственном уровне в лице принятия и подписания Ханойской конвенции, предстоит ещё много работы, как при внесении изменений в действующее отечественное законодательство (в части виртуальных активов и электронных доказательств прежде всего), так и при разработке дополнительных протоколов. Хотя последнее может рассматриваться только примерно через полтора года (после вступления в силу на 90-ый день после сдачи 40 ратификационной грамоты или приравненного к ней документа и созыва Конференции государств-участников в течение года после этого), уже сейчас важно прорабатывать консолидированную позицию стран

[4] 12.11.2025.

Глобального Юга фактически в противовес «закрытому клубу» западных демократий и Глобальному Северу.

Список источников и литературы:

1. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. – 2022. – № 4. – С. 88-94.
2. Бессонов А. А. О некоторых направлениях совершенствования криминалистического обеспечения расследования киберпреступлений // Расследование преступлений: проблемы и пути их решения. – 2024. – № 2(44). – С. 31-37.
3. Генеральная Ассамблея ООН: Резолюция 79/243, принятая Генеральной Ассамблеей 24декабря 2024 года «Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям» [Электронный ресурс] // ООН. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 12.11.2025).
4. Конвенция Организации Объединенных Наций против коррупции [Электронный ресурс] // ООН. URL: https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml pdf (дата обращения: 12.11.2025).
5. Конвенция Организации Объединенных Наций против транснациональной организованной преступности [Электронный ресурс] // ООН. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения: 12.11.2025).
6. Литвишко П. А. Первый глобальный договор против киберпреступности: от геополитической конфронтации к профессиональному компромиссу // Международная жизнь. – 2024. – № 1. – С. 1–27.
7. Литвишко П. А., Михалева Е.С. Состояние и перспективы электронного взаимодействия при оказании международной правовой помощи по уголовным делам и правоохранительного содействия // Вестник Университета прокуратуры Российской Федерации. – 2022. – № 2(88). – С. 130-144.
8. Оговорки к Конвенции Организации Объединенных Наций против коррупции [Электронный ресурс] // Коллекция международных договоров ООН. URL: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-14&chapter=18&clang=_en#EndDec (дата обращения: 12.11.2025).

9. Оговорки к Конвенции Организации Объединенных Наций против транснациональной организованной преступности [Электронный ресурс] // Коллекция международных договоров ООН. URL: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en (дата обращения: 12.11.2025).
10. Поляков И. С. Процессуальное оформление действий, направленных на фиксацию криминалистически значимой информации в информационнотелекоммуникационных сетях: современное состояние // Применение уголовного и уголовно-процессуального законодательства в практике Следственного комитета Российской Федерации: актуальные проблемы и рекомендации по их решению : Материалы Всероссийской научно-практической конференции, Екатеринбург, 21–22 мая 2024 года. – Москва: Московская академия следственного комитета, 2024. – С. 101-106.
11. Рекомендации ФАТФ [Электронный ресурс] // ЕАГ. URL: https://eurasiangroup.org/files/uploads/files/other_docs/FATF%20docs/rekomendacii-fatf-2019.pdf (дата обращения: 12.11.2025).
12. Руководство по применению риск-ориентированного подхода в отношении виртуальных активов и провайдеров виртуальных услуг [Электронный ресурс] // Центральный банк России. URL: https://cbr.ru/content/document/file/113302/Руководство_РОП_ВА_ПУВА.pdf (дата обращения: 12.11.2025).
13. Цыплакова А. Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности // Российский следователь. – 2025. – № 10. – С. 62-66.
14. Яссин А. А. Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств // Journal of Digital Technologies and Law. – 2024. – № 2 (2). – С. 262-285.
15. Цыплакова А. Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: современное состояние, проблемы и перспективы // Право и управление. XXI век. – 2025. – Т. 21. – № 3(76). – С. 62-75.
16. Advancing the UN Global Intergovernmental Points of Contact (PoC) Directory [Электронный ресурс] // UN TV. 15.10.2025. URL: https://webtv.un.org/en/asset/k12/k12ubrh6iv (дата обращения: 04.11.2025).
17. بيان وفد سلطنة عمان [Заявление делегации Султаната Оман] [Электронный ресурс] // УНП ООН. URL:

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/_002.pdf (дата обращения: 12.11.2025).

18. قانصو علي. الحرب الإلكترونية // مجلة الدفاع الوطني البناني. ٢٠٢١. ١١٨. ٣-٣٥ ص [Кансо Али. Электронная война // Журнал национальной обороны Ливана. – 2021. – № 118. – С. 3–35].

19. ليلى ميسوم. المخدرات الرقمية: ظهور إدمان جديد عبر شبكة الإنترنت // مجلة جيل العلوم الإنسانية والاجتماعية. ٢٠١٢. ٢١. ١٦٣-١٧٤ ص [Лейла Мессум. Цифровые наркотики: Возникновение новой онлайн-зависимости // Журнал «Поколение гуманитарных и социальных наук». – 2012. № 21. – С. 163-174].

Аревик Жораевна Мартиросян,
к.ю.н., научный сотрудник ИАМП, руководитель Школы МИБ ИАМП,
доцент кафедры государственного управления,
Дипломатическая академия МИД России,
E-mail: a.martirosian@dipacademy.ru

Arevik Zh. Martirosyan,
Ph.D, in Law, Researcher, Institute of Contemporary International Studies,
Head of the International Information Security School,
Associate Professor, Department of Public Administration,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: a.martirosian@dipacademy.ru

ЦИФРОВАЯ ПОВЕСТКА И ЕЕ ИТОГИ В 2025 ГОДУ: МЕЖДУНАРОДНО-ПРАВОВАЯ ТРАНСФОРМАЦИЯ И ГЕОПОЛИТИЧЕСКИЕ ВЕКТОРЫ

DIGITAL AGENDA AND ITS OUTCOMES IN 2025: INTERNATIONAL LEGAL TRANSFORMATION AND GEOPOLITICAL VECTORS

Аннотация. Представлены международно-правовые и геополитические итоги 2025 года, связанные с ключевыми цифровыми треками: международной информационной безопасностью, борьбой с киберпреступностью, интернет-управлением и искусственным интеллектом. Освещены организационные реформы в системе ООН, включая запуск новых механизмов, принятие первой универсальной международной конвенции по противодействию киберпреступности и институционализацию цифровой повестки как элемента международной безопасности и сотрудничества.

Ключевые слова: международное право, ООН, ИКТ, цифровая повестка, международная информационная безопасность, киберпреступность, WSIS, искусственный интеллект, международное регулирование ИИ, управление ИИ.

Abstract. The article presents the international legal and geopolitical outcomes of 2025 related to key digital tracks: international information security, combating cybercrime, internet governance, and artificial intelligence. It highlights organizational reforms within the UN system, including the launch of new mechanisms, the adoption of the first universal international convention on combating cybercrime, and the institutionalization of the digital agenda as an element of international security and cooperation.

Keywords: international law, UN, ICT, digital agenda, international information security, cybercrime, WSIS, artificial intelligence, international AI regulation, AI governance.

2025 год закрепил переход цифровой повестки от фрагментарных инициатив и регулирования, основанного на нормах «мягкого права», к более устойчивым, институционально оформленным механизмам в системе ООН. Это касается как

проблематики международной информационной безопасности, так и управления интернетом и искусственным интеллектом. Ряд ключевых процессов под эгидой ООН достигли важнейших решений, которые переводят цифровую тематику из разряда дискуссий в плоскость конкретных механизмов сотрудничества с четко определенным мандатом и определенного международно-правового регулирования.

Трек международной информационной безопасности. В сфере международной информационной безопасности завершилась работа второго созыва Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021-2025), учреждённой резолюцией ГА ООН 75/240. Она открыла путь к созданию постоянно действующего глобального механизма координации усилий государств – Всемирного механизма по достижениям в области ИКТ в контексте международной безопасности и продвижению ответственного поведения государств в сфере использования ИКТ. Летом 2025 года группа единогласно одобрила итоговый доклад, в котором рекомендовала создать постоянно действующий механизм в рамках ООН для продолжения многостороннего сотрудничества по международной информационной безопасности. Генеральная Ассамблея ООН поддержала эту инициативу, и новый орган получил мандат, охватывающий весь комплекс вопросов, ранее рассматриваемых в формате РГОС. Таким образом, произошла трансформация от «ad hoc» (временных) переговорных механизмов к постоянной институциональной архитектуре, которая начнет свое функционирование в 2026 году [3].

Трек борьбы с киберпреступностью. По итогам деятельности Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях состоялось принятие итогового текста Конвенции ООН по противодействию киберпреступности [2]. Ее подписание в октябре 2025 года стало одним из ключевых юридических итогов цифровой повестки и важным шагом в сторону универсализации международно-правового регулирования ИКТ-среды. Значение Конвенции заключается в следующем:

– создание универсальной договорной базы для международного сотрудничества в сфере противодействия преступному использованию ИКТ;

– институционализация механизмов международной правовой помощи и процессуального взаимодействия;

– переход от региональной фрагментации к глобальному правовому инструменту (ее принятие заполнило важный пробел в международном праве: ранее борьба с

киберпреступностью основывалась на разрозненных региональных соглашениях, тогда как теперь заложена единая правовая основа для международного сотрудничества).

Трек управления интернетом или итоги обзора WSIS+20 – от повестки развития к комплексному цифровому управлению. В декабря 2025 года состоялся обзор реализации решений WSIS+20, который подтвердил устойчивость повестки информационного общества, но одновременно зафиксировал необходимость ее качественного обновления. Ключевые итоги WSIS+20:

– сохранение WSIS как рамочной платформы цифрового развития в системе ООН;

– усиление взаимосвязи между вопросами развития, управления интернетом и безопасности;

– признание роли ИИ, данных и платформенных экосистем как факторов социально-экономической трансформации;

– «придание Форуму по управлению Интернетом (Internet Governance Forum, IGF) статуса постоянного механизма системы ООН. Тем самым завершен этап мандатного продления (2005, 2010, 2015 гг.) и закреплена долгосрочная роль IGF как многостейкхолдерной площадки для диалога по вопросам управления Интернетом» [1].

– необходимость лучшей координации между WSIS, IGF и новыми институциональными механизмами в цифровой сфере.

Кроме того, «итоговый документ подтверждает архитектуру WSIS и ориентирован на повышение согласованности цифровых процессов в системе ООН. В частности, предусмотрена разработка целевых «дорожных карт» WSIS с увязкой с Целями устойчивого развития и Глобальным цифровым договором» [1].

Показательно, что было принято решение придать IGF статус постоянной институции, что запустило процесс его реформирования и укрепления и соотносится с тенденцией на создание постоянно действующих механизмов в цифровой сфере.

Трек управления искусственным интеллектом. Отдельного внимания заслуживает институционализация глобального управления ИИ, которая в 2025 году вышла на качественно новый уровень. Под эгидой ООН ускоренно вырабатываются процедурные и организационные механизмы, переходя от прежних деклараций к конкретным шагам. Кульминацией стал август 2025 года, когда Генассамблея ООН приняла резолюцию A/RES/79/325, предусматривающую создание и запуск новых межправительственных (Глобального диалога по управлению ИИ) и экспертных органов (Независимой международной научной панели по ИИ) по ИИ под эгидой ООН.

Однако процесс сопровождается нарастающей политизацией: множественность параллельных инициатив и разногласия по содержанию документов указывают на риск

нормативной раздробленности и конкуренции режимов регулирования. Тем не менее наблюдается постепенное смещение от этических деклараций к институциональным механизмам координации и надзора. Данные процессы свидетельствуют о признании ИИ не только технологическим, но и политико-правовым феноменом, требующим отдельной архитектуры глобального управления.

Заключение. Реорганизация РГОС, принятие Конвенции по киберпреступности, итоги WSIS+20 и формирование новых органов по ИИ разворачиваются на фоне усиливающейся геополитической конкуренции. Цифровая повестка в своей совокупности все отчетливее выступает:

– пространством конкуренции моделей регулирования;

– инструментом стратегического влияния;

– фактором перераспределения власти в системе международных отношений.

Достигнутые в 2025 году договоренности обозначили лишь веху на пути формирования глобального цифрового порядка, и впереди стоит большая работа по их реализации и развитию. Во-первых, необходима институциональная согласованность: преодоление разрозненности существующих механизмов и объединение усилий разных площадок. Отсутствие унифицированного международно-правового режима, регулирующего поведение государств в цифровом пространстве, уже породило фрагментацию подходов и затруднило выработку согласованных принципов и обязательств. Теперь, когда появились новые органы (постоянный механизм ООН по безопасности ИКТ, глобальный диалог по ИИ, обновленная архитектура WSIS и IGF), важно выстроить их работу во взаимодополняющем режиме, исключив дублирование мандатов и противоречие в рекомендациях. Во-вторых, критично обеспечить преемственность и преодолеть институциональную разобщенность в ООН: «межведомственные» механизмы, такие как Группа ООН по информационному обществу (UNGIS), уже сейчас работают над повышением согласованности политики различных агентств ООН в цифровой сфере, и эта работа должна быть усилена. В перспективе следующего этапа приоритетом станет реализация принятых обязательств и мониторинг исполнения. 2025 год заложил фундамент новой системы – впереди её институциональная настройка, нормативное наполнение и закрепление механизмов международного взаимодействия.

Список источников и литературы:

1. ГА ООН приняла итоговый документ WSIS+20 [Электронный ресурс] // Telegram : канал «Школа международной информационной безопасности Института актуальных международных проблем Дипломатической академии МИД России». URL: https://t.me/iis_mib_school/1249 (дата обращения: 20.12.2025).

2. Конвенция Организации Объединенных Наций против киберпреступности (резолюция Генеральной Ассамблеи ООН 79/243) [Электронный ресурс] // ООН, 2025. URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 15.01.2026).

3. Мартиросян А. Ж. Точка перехода: от рабочих и экспертных групп к постоянному механизму ООН по вопросам обеспечения безопасности в сфере использования ИКТ // РСМД. 2025. 2 сент. URL: https://russiancouncil.ru/analytics-and-comments/analytics/tochka-perekhoda-ot-rabochikh-i-ekspertnykh-grupp-k-postoyannomu-mekhanizmu-oon-po-voprosam-obespech/ (дата обращения: 20.12.2025).

Секция B1
«Национальные и региональные траектории цифрового суверенитета и информационной безопасности»

Антипов Даниил Романович,
магистрант,
Дипломатическая академия МИД России,
E-mail: daniil.antipov@icloud.com

Daniil R. Antipov,
Master's student,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: daniil.antipov@icloud.com

ЕВРОАТЛАНТИЧЕСКОЕ ИЗМЕРЕНИЕ ЦИФРОВОЙ ПОЛИТИКИ И КИБЕРБЕЗОПАСНОСТИ ФРАНЦИИ

EURO-ATLANTIC DIMENSION OF FRANCE'S DIGITAL POLICY AND CYBERSECURITY

Аннотация. В статье поставлен вопрос о том, какое место в цифровой стратегии Франции занимают Европейский союз и НАТО. Проанализировано участие Пятой республики в выработке европейских мер регуляции использования передовых технологий и работы бизнеса в исследуемой отрасли; корреляция её подхода к проведению операций в информационном и кибернетическом пространствах с доктринальными положениями и усилиями НАТО и США. Отмечается решающее значение опоры на евроатлантических союзников для обеспечения кибербезопасности Франции.

Ключевые слова: Франция, ЕС, НАТО, кибербезопасность, регуляторные меры, информационные операции, сотрудничество.

Abstract. The article raises the question what place the European Union and NATO occupy in France's cybersecurity strategy. The author analyzes the French participation in the development of European measures to regulate the advanced technologies use and business activities in the industry under study; the correlation of its approach to operations conducting in information and cyberspace with doctrinal provisions and measures of NATO and the US. The crucial importance of relying on Euro-Atlantic allies to ensure France's cybersecurity is noted.

Key words: France, EU, NATO, cybersecurity, regulatory measures, information operations, cooperation.

Стремительно меняющаяся международная среда испытывает влияние наступления новой фазы технологического развития, на которой высокие технологии становятся одной из составляющих, а потенциально – основой глобального экономического, политического

и иного влияния. Сулящим значительные перспективы переходным этапам развития человечества одновременно диалектически имманентно появление принципиально новых вызовов и угроз. Ныне информационное и кибернетическое пространства образуют как поле межгосударственного сотрудничества, так и арену конкуренции, противостояния и даже борьбы главных акторов и «творцов» мирового порядка, стремящихся использовать потенциал прорывных средств, обеспечить внутренний контроль над ними и предотвратить их деструктивное применение извне. В данном контексте непосредственную важность обретает анализ страновых подходов к обеспечению информационной безопасности.

Франция является одним из двух (наряду с Германией) наиболее весомых игроков в Европейском союзе, державой, обладающей заметным политическим, экономическим и идейно-ценностным ресурсом на глобальном уровне. Вместе с тем, как отметили французские аналитики Жан-Луи Жергорен и Лео Исаак-Доньян, ни одна даже крупная европейская страна «несмотря на превосходный качественный уровень кибер-возможностей… не в состоянии по отдельности потягаться с превосходящими средствами США, России и Китая» [6]. Вследствие этого Франция видит основу своей стратегической автономии в опоре на ближайших союзников по ЕС и НАТО [12], составляющих, таким образом, главное международное измерение её цифровой политики и кибербезопасности.

Франция в авангарде выработки регуляторных мер ЕС для киберпространства. На текущей стадии развития норм и стандартов в сфере регламентации использования новейших технологий и деятельности цифровых корпораций ЕС добивается правовой конвергенции в этих областях, что позволит ему преобразоваться в «нечто большее, чем только сумма» своих национальных компонент [8]. Евросоюз также поощряет цифровизацию масштабными инвестициями. Последнее особо актуально для Франции, интенсифицирующей усилия по стимулированию различных технологических «стартапов» [13]. Их потенциал могут усилить вливания не только национальных, но и европейских средств. Но отметим, что интерес Парижа выходит далеко за пределы получения финансирования от структур Евросоюза и заключается в том, чтобы стать во главе процессов внедрения и законодательного регулирования передовых технологий.

Эволюция позиции Франции по вопросу формирования общей политики Евросоюза в цифровой сфере соответствует поступательному развитию данного направления на наднациональном уровне. Более того, каждый новый шаг французской дипломатии носит инициирующе-предвещающий характер. Так, в Стратегии Франции в области защиты и безопасности информационных систем 2011 г. заявлялось, что страна будет активно участвовать в разработке политики киберзащиты ЕС [11]. Последнюю вскоре

концептуализировали Стратегией кибербезопасности ЕС 2013 г. и Рамочной концепцией ЕС о защите от киберугроз 2014 г. [2, с. 143].

Далее, в Национальной стратегии цифровой безопасности 2015 г. Франция возложила на себя задачу стать вместе с другими добровольцами из рядов ЕС движущей силой европейской цифровой стратегической автономии и способствовать регуляции, стандартизации и сертификации исследований и разработок в отрасли с особым акцентом на недопущение технологической и экономической зависимости Европы и отчуждения личных персональных и конфиденциальных корпоративных данных [18]. Эти и другие идеи (например, из французского Закона о военном планировании 2013 г.) были отражены в Директиве ЕС по вопросам безопасности сетей и инфраструктуры 2016 г. [10, с. 9].

Наконец, в документах действующей президентской администрации: Международной стратегии Франции в цифровой сфере 2017 г., Стратегическом обзоре кибероборонны 2018 г. и Национальной стратегии кибербезопасности 2023 г. – особое внимание уделено вопросу конкурентоспособности ЕС в глобальном масштабе в информационной и кибернетической сферах, становления союза как самодостаточного в промышленном отношении актора [1, с. 160]. Этой и иной проблематике, относящейся к «киберсуверенитету», посвящен, в частности, ежегодно проводимый во Франции форум European Cyber Week, который в 2025 г. состоялся 17-20 ноября [9].

Достижение целей суверенитета и конкурентоспособности предполагает серьезную институциональную работу. Обратимся к текущему взаимодействию отвечающего за это Агентства национальной безопасности информационных систем Франции (Agence nationale de la sécurité des systèmes d'information, ANSSI) со структурами ЕС. В ныне действующем Стратегическом плане на 2025-2027 гг. выделено четыре направления сотрудничества:

1. Участие в разработке стандартов и регуляторных мер на основании Директивы ЕС о безопасности сетей и информационных систем 2023 г. (Network and Information Security Directive 2, NIS 2), Закона ЕС о киберустойчивости 2024 г. (Cyber Resilience Act, CRA), Закона ЕС об искусственном интеллекте 2024 г. (AI Act), Схемы сертификации кибербезопасности ЕС, основанной на общих критериях 2025 г. (EU Cybersecurity Certification Scheme based on Common Criteria, EUCC), в рамках Европейской группы по сотрудничеству в области цифровой идентификации (European Digital Identity Cooperation Group, EDICG). В частности, ANSSI участвовала в пересмотре регламента электронной идентификации ЕС eIDAS и в рабочих группах по его техническому внедрению, поддерживая более широкий учет аспектов кибербезопасности [15].

2. Поддержка развития единого, динамичного и заслуживающего доверие рынка цифровых продуктов и услуг с одновременным продвижением французской модели

сертификации услуг: пересмотр Закона ЕС о кибербезопасности 2024 г. (Cybersecurity Act, CSA).

3. Содействие сотрудничеству в укреплении киберустойчивости и, в частности, намерение организовывать международные антикризисные учения с использованием существующих сетей.

4. Поощрение новых форм публичных действий в киберпространстве на европейском уровне на основе опыта реализации плана экономического стимулирования France Relance и Парижских Олимпийских игр 2024 г. [14].

В ходе своего председательства в совете ЕС в первой половине 2022 г. Франция поспособствовала принятию двух новых законодательных актов ЕС, регулирующих деятельность цифровых гигантов: первый – Закон о цифровых рынках (Digital Markets Act, DMA), запрещающий навязывать потребителям программное обеспечение и использовать персональные данные в рекламных целях (в случае нарушения предусмотрен штраф в размере до 10% от оборота компании), и второй – Закон о цифровых услугах (Digital Services Act, DSA), позволяющий государствам получать доступ к алгоритмам крупных цифровых платформ для борьбы с преступными материалами [16, с. 12]. Эти акты дали ЕС больший инструментарий вмешательства в дела частного цифрового сектора, особенно крупных американских компаний, продолжив логику французского налога GAFA, вводившего 3% налог на прибыль цифровых гигантов.

Также Франция осуществляет адаптацию национального законодательства в соответствии с обозначенными актами. В 2024 г. агентство ANSSI начало работу по внедрению CRA, запустив проект по организации отчетности об уязвимостях и инцидентах [15]. Кроме того, директива NIS 2 конкретизировала классификацию основных предприятий, подверженных риску. К внесению изменений во французское законодательство привело и принятие Общего регламента ЕС по защите данных (General Data Protection Regulation, GDPR) в 2018 г. Однако, как отметили французские эксперты по кибербезопасности Пьер Аффагар и Матильда Карвес, в большинстве случаев европейские нормативные акты не влияют на французское законодательство, ведь чаще оно превышает стандарты, установленные ЕС. К примеру, Франция первая в союзе на экспериментальной основе узаконила алгоритмическое видеонаблюдение, а также, в отличие от других государств-членов, пошла дальше рамок ЕС в отношении обязательств и ограничений для бизнеса, связанных с кибербезопасностью: Закон о руководстве и планировании Министерства внутренних дел № 2023-22 от 24 января 2023 г. (Loi d'Orientation et de Programmation du Ministère de l'Intérieur, LOPMI) и Закон о защите и регулировании цифрового пространства № 2024-449 от 21 мая 2024 г. (Loi Visant à Sécuriser et à Réguler

l'Espace Numérique, SREN). Наиболее примечательным последствием последнего стал арест Павла Дурова [7].

Все это гармонизирует юридические рамки использования передовых технологий на национальном французском и наднациональном европейском уровнях, повышая степень гомогенности организации и, следовательно, обеспечивая возможность однонаправленных и согласованных действий.

Отражение «атлантических» установок во французском подходе к обеспечению кибербезопасности. На следующей после ЕС ступени в международных приоритетах Франции в цифровой сфере стоит Североатлантический альянс. Взаимодополняемость усилий двух организаций, интеграция мер по киберзащите в их операции на непротиворечивой основе считается одним из основных элементов их взаимодействия, обеспечивающим рациональность приложения усилий. Этот принцип, конкретизированный для сферы кибербезопасности, был воспроизведен 22 сентября 2023 г. на встрече высокопоставленных должностных лиц НАТО и ЕС [19].

В целом страны Организации Североатлантического договора оперируют во многом идентичными концептуально-стратегическими установками и реализуют схожую в организационно-техническом отношении тактику [3, с. 162]. Основополагающим совпадением подходов НАТО и Франции к обеспечению кибербезопасности является их готовность вести не только оборонительные (реактивные), но и наступательные (проактивные) операции [1, с. 159, 162], [4].

Кроме того, Франция является полноправным участником ежегодно проводимых учений Cyber Coalition [5]. Примечательно, что в 2018 г. французская высшая военная школа выступила в качестве места проведения Конференции НАТО по кибербезопасности [17], что свидетельствовало о стремлении Пятой республики быть на передовой развития этого направления. Франция наравне с Данией, Нидерландами и Норвегией принадлежит и к такому неформальному объединению в области сигнальной разведки, как альянс «Девять глаз» (Nine Eyes), расширенному партнерству «пятерки», «ядра» в лице государств англосферы. Обратим внимание, что, например, Германия принадлежат уже к формату (Fourteen Eyes) [3, с. 172-173], что также характеризует заметно более высокое положение Франции в числе европейских союзников США в данной сфере.

В рамках НАТО Париж добился заметных успехов в деле объединения усилий по обеспечению интересов и безопасности в киберпространстве. Франция еще в 2016 г. на саммите организации в Варшаве инициировала принятие общих «Обязательств по киберзащите» [12]. Тогда же страны альянса признали киберпространство одной из сфер проведения его операций. В 2018 г. НАТО согласовала пути интеграции деятельности по

обеспечению кибербезопасности на уровне отдельных национальных государств-членов и приняли решение создать общий Центра кибероперацій [3, с. 163]. В 2023 г. в ходе саммита в Вильнюсе на основе прежний решений была выработана более амбициозная концепция киберзащиты как одного из элементов сдерживания и общей обороны НАТО, а также запущен механизм взаимной поддержки в случае «виртуальных киберинцидентов» (Virtual Cyber Incident Support Capability, VCISC). В 2024 г. участники саммита НАТО в Вашингтоне договорились создать Интегрированный центр киберзащиты [1, с. 161]. Таким образом, Франция стояла у истоков развивающейся в наши дни стратегии НАТО в сфере информационной борьбы.

Заключение. Париж в полной мере использует возможности партнерства со своими евроатлантическими союзниками на полях ЕС и НАТО. В Евросоюзе Париж занимает лидирующие позиции в выработке общего стратегического видения и формировании регуляторных мер в цифровой области и сфере кибербезопасности. Страна развивает национальное законодательство, не только адаптируясь под регламенты Евросоюза, но и во многом опережая его политику, впоследствии применяя свой опыт на межгосударственном уровне. Стратегии Франции и НАТО по реализации информационного противоборства являются, по сути, конвергентными. Взаимодействие с атлантическими союзниками позволяет Парижу как участвовать в совместных мероприятиях, направленных на повышение устойчивости стран блока к информационным атакам, так и продвигать свои идеи, в конечном счете обеспечивая взаимосвязь и взаимодополняемость усилий Североатлантического альянса и Европейского союза.

Список источников и литературы:

1. Антипов Д.Р. Средства информационного противоборства во внешнеполитическом арсенале Франции // Россия и мир: диалоги – 2025. Стратегии: IX Международная научно-практическая конференция (22-23 мая 2025 г.) – М.: Национальный исследовательский институт развития коммуникаций, 2025. – С. 158-163.
2. Верхелст Э., Ваутерс Я. Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. 2020. №2. С. 141-172.
3. Манойло А.В. Современные стратегии кибербезопасности и кибероборонь НАТО // АПЕ. 2020. №3. С. 160-184.
4. Approche de l’OTAN pour la lutte contre les menaces informationnelles // North Atlantic Treaty Organization. 16 janvier 2025. URL: https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=fr (consulté le 11.11.2025)

5. Cyber Coalition: NATO’s Flagship Cyber Exercise // Allies Command Transformation. NATO’s Strategic Warfare Development Command. 2024. URL: https://www.act.nato.int/activities/cyber-coalition/ (accessed: 11.05.2025)
6. « Cyber. La guerre permanente » – 3 questions à Jean-Louis Gergorin et Léo Isaac-Dognin // IRIS. 4 janvier 2019. URL: https://www.iris-france.org/127540-cyber-la-guerre-permanente-3-questions-a-jean-louis-gergorin-et-leo-isaac-dognin/ (consulté le 11.11.2025)
7. Cybersecurity Laws and Regulations France 2025 // ICLG. November 6, 2024. URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/france (accessed: 11.05.2025)
8. EU Cybersecurity Strategy // European Commission. 2020. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (accessed: 11.05.2025)
9. European Cyber Week 2025 : J-14 avant le grand rendez-vous de la cyber en France ! // Commandement de la cyberdéfense. 3 novembre 2025. URL: https://www.defense.gouv.fr/comcyber/actualites/european-cyber-week-2025-j-14-grand-rendez-vous-cyber-france (consulté le 11.11.2025)
10. Hathaway M., Demchak Ch., Kerben J., McArdle J., Spidalieri F. France Cyber Readiness at a Glance. – Arlington (VA): Potomac Institute for Policy Studies, 2016. – 27 p.
11. Information systems defence and security France’s strategy // Agence nationale de la sécurité des systèmes d'information. February, 2011. URL: https://cyber.gouv.fr/sites/default/files/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (accessed: 11.05.2025)
12. La stratégie internationale de la France pour le numérique // Ministère de l’Europe et des Affaires étrangères. 2017. URL: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-strategie-internationale-de-la-france-pour-le-numerique/ (consulté le 11.11.2025)
13. National Cybersecurity Strategy // Secrétariat général pour l’investissement du Gouvernement. France 2030. 2023. URL: https://project.inria.fr/FranceJapanICST/files/2023/10/Présentation-SN-CY-EN-v2.pdf. (accessed: 11.05.2025)
14. Plan stratégique de l’Agence nationale de la sécurité des systèmes d’information 2025-2027 // Agence nationale de la sécurité des systèmes d'information. 6 mars 2025. URL: https://cyber.gouv.fr/strategie (consulté le 11.11.2025)
15. Rapports d’activités // Agence nationale de la sécurité des systèmes d'information. 15 avril 2025. URL: https://cyber.gouv.fr/rapports-dactivites (consulté le 11.11.2025)

16. Results of the French Presidency of the Council of the European Union // France22: French Presidency of the Council of the European Union. 2022. 21 p.

17. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militaire, Paris) // North Atlantic Treaty Organization. May 15, 2018. URL: https://www.nato.int/cps/en/natohq/opinions_154462.htm?selectedLocale =ru (accessed: 11.05.2025)

18. Strarégie nationale pour la sécurité du numérique // Agence nationale de la sécurité des systèmes d'information. 2015. URL: https://cyber.gouv.fr/sites/default/files/document/strategie_nationale_securite_numerique_fr.pdf (consulté le 11.11.2025)

19. The European Union and NATO intensify cooperation on addressing cyber threats // The Diplomatic Service of the European Union. September 22, 2023. URL: https://www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en (accessed: 11.05.2025)

Серафим Юрьевич Архипенко,
курсант 4 курса военного факультета в Белорусском государственном университете,
E-mail: s.arkhipenka@yandex.by

Serafim Arkhipenka,
4th year cadet of the Military Faculty at the Belarusian State University,
E-mail: s.arkhipenka@yandex.by

ЦИФРОВОЙ СУВЕРЕНИТЕТ КАК ОСНОВА НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DIGITAL SOVEREIGNTY AS THE BASIS OF NATIONAL AND INTERNATIONAL INFORMATION SECURITY

Аннотация. Цифровой суверенитет становится ключевым элементом обеспечения национальной и международной информационной безопасности в эпоху стремительной цифровизации и роста киберугроз. Он определяется как право и способность государства самостоятельно управлять своей цифровой инфраструктурой, информационными потоками и данными, защищая их от внешнего вмешательства и кибератак. В современных международных отношениях цифровой суверенитет становится не только технической, но и политической и экономической задачей, влияющей на национальную безопасность, экономическую независимость и суверенитет личности. Особое значение приобретают регулирование и создание национальных стандартов в области цифровых технологий, защита цифровой инфраструктуры, а также международное сотрудничество для противодействия глобальным киберугрозам.

В докладе рассматриваются основные принципы цифрового суверенитета: автономия данных и технологий, контроль над хранением и обработкой информации, использование отечественных программных средств и аппаратных решений, а также законодательное регулирование и международное сотрудничество. Акцент делается на вызовах, связанных с глобализацией цифровых ресурсов, санкционными рисками и необходимостью адаптации к новым геополитическим реалиям.

Цель доклада – показать, как цифровой суверенитет может стать фундаментом для устойчивой национальной и международной информационной безопасности, способствуя развитию национальных ИТ-индустрий, укреплению международного сотрудничества и обеспечению защиты информации в условиях растущих вызовов цифровой эпохи.

Ключевые слова: цифровой суверенитет, информационная безопасность, национальная безопасность, международные отношения, кибербезопасность, цифровая инфраструктура, законодательное регулирование, геополитика.

Abstract. Digital sovereignty is becoming a key element of ensuring national and international information security in an era of rapid digitalization and the growth of cyber threats. It is defined as the right and ability of the state to independently manage its digital infrastructure, information flows and data, protecting them from external interference and cyberattacks. In modern international relations, digital sovereignty is becoming not only a technical, but also a political and economic task that affects national security, economic independence, and individual sovereignty. Regulation and creation of national standards in the field of digital technologies, protection of digital infrastructure, as well as international cooperation to counter global cyber threats are of particular importance.

The report examines the basic principles of digital sovereignty: the autonomy of data and technology, control over the storage and processing of information, the use of domestic software and hardware solutions, as well as legislative regulation and international cooperation. The focus is on the challenges associated with the globalization of digital resources, sanctions risks, and the need to adapt to new geopolitical realities.

The purpose of the report is to show how digital sovereignty can become the foundation for sustainable national and international information security, contributing to the development of national IT industries, strengthening international cooperation and ensuring information protection in the face of the growing challenges of the digital age.

Key words: digital sovereignty, information security, national security, international relations, cybersecurity, digital infrastructure, legislative regulation, geopolitics.

Под цифровым суверенитетом в широком смысле следует понимать право и способность государства самостоятельно формировать политику в цифровой сфере и обеспечивать контроль над ключевыми цифровыми ресурсами: инфраструктурой, данными, информационными потоками и критическими технологиями.

Цифровой суверенитет включает несколько взаимосвязанных измерений: технологическое измерение – обладание и развитие собственных технологий, инфраструктуры и компетенций; правовое измерение – разработка и применение национального законодательства, регулирующего цифровое пространство; политическое измерение – способность отстаивать свои интересы в международных цифровых форматах; экономическое измерение – снижение зависимости от внешних поставщиков цифровых

услуг и оборудования; социально-гуманитарное измерение – защита прав и свобод граждан в цифровой среде, суверенитет личности над собственными данными [3].

В современных условиях можно выделить несколько базовых принципов цифрового суверенитета, вокруг которых строится национальная политика и международное взаимодействие.

1. Автономия данных и технологий

Автономия данных включает: контроль над сбором, хранением и обработкой данных граждан, организаций и государственных органов; установление правил трансграничной передачи данных; развитие национальных и региональных хранилищ данных, облачных решений и дата-центров.

2. Контроль над хранением и обработкой информации

Контроль над данными не означает изоляцию, но предполагает: прозрачные и предсказуемые механизмы доступа к данным для государственных органов при соблюдении прав граждан; четкие требования к локализации данных и использованию иностранных облачных сервисов; защиту внутренних информационных потоков от несанкционированного внешнего доступа, включая шпионское ПО, кибершпионаж, недобросовестное использование алгоритмов обработки данных.

3. Развитие отечественного программного обеспечения и аппаратных решений: повышает прозрачность технологической цепочки (supply chain security); снижает риски скрытых уязвимостей и преднамеренных закладок; создает стимулы для развития национальной ИТ-индустрии, образования и науки. При этом важно уделять внимание не только разработке, но и всему жизненному циклу продуктов.

4. Законодательное регулирование и институциональная архитектура: законодательство должно быть технологически нейтральным, гибким и адаптивным, чтобы не тормозить инновации и в то же время обеспечивать высокий уровень защиты.

5. Международное сотрудничество: цифровой суверенитет не может пониматься как полная изоляция. Речь идет о суверенном участии в глобальных процессах на основе равноправия и взаимного уважения [1].

Вызовы и риски в условиях глобализации и санкционного давления. Реализация цифрового суверенитета сталкивается с рядом серьезных вызовов. Во-первых, глобализация цифровых ресурсов и услуг привела к концентрации данных и сервисов в руках ограниченного числа транснациональных корпораций. Это создает асимметрию: многие государства оказываются «пассивными потребителями», не имеющими доступа к исходному коду, алгоритмам и архитектуре используемых ими решений.

Во-вторых, санкционные режимы и геополитическая конфронтация усиливают роль цифровой зависимости как инструмента давления. Ограничения в доступе к оборудованию, программному обеспечению, обновлениям и сервисам несут не только экономические, но и прямые риски для национальной безопасности.

В-третьих, существует риск фрагментации глобального цифрового пространства на изолированные региональные или национальные сегменты. Это может затруднить международное сотрудничество, тормозить инновации и усугублять недоверие между государствами [2].

Цифровой суверенитет как драйвер развития. Важно подчеркнуть, что цифровой суверенитет – это не только оборонительный щит, но и мощный стимул развития. Во-первых, он мотивирует создание национальных инновационных экосистем в области ИТ, кибербезопасности, телекоммуникаций и электроники. Во-вторых, формирует спрос на высокотехнологичные продукты и услуги, поддерживая рост квалифицированной занятости и развитие человеческого капитала. В-третьих, способствует диверсификации экономики и снижению зависимости от сырьевых отраслей, создавая новые экспортно-ориентированные сегменты. При этом важен баланс: политика импортозамещения и поддержки отечественных решений должна сочетаться с интеграцией в глобальные научно-технологические сети, участием в международных стандартах и проектах [4].

Заключение. Цифровой суверенитет становится системообразующим элементом современной архитектуры национальной и международной информационной безопасности. Он объединяет технологические, правовые, экономические и гуманитарные измерения, определяя способность государств защитить свои интересы и права граждан в цифровую эпоху. Речь не идет о самоизоляции или создании «цифровых стен». Задача состоит в том, чтобы обеспечить устойчивость и управляемость цифрового развития, сформировать справедливые и безопасные правила игры в глобальном киберпространстве, основанные на принципах суверенитета, равноправия и сотрудничества. Цифровой суверенитет, реализованный на этих принципах, может и должен стать фундаментом устойчивой национальной и международной информационной безопасности, содействовать развитию национальных ИТ-индустрий, укреплению доверия между государствами и защите человека в условиях растущих вызовов цифровой эпохи.

Список источников и литературы:

1. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности [Электронный ресурс] // Вестник МГИМО, 2016;(6(51)):76-91. URL: https://www.vestnik.mgimo.ru/jour/article/view/640?locale=ru_RU (дата обращения: 11.12.2025).

2. Цифровой суверенитет как залог глобальной безопасности [Электронный ресурс] // Российский международный форум «Знание». URL: https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti/ (дата обращения: 11.12.2025).

3. NIS 2 And Europe's Digital Sovereignty a Strategy for Secure Digital Infrastructure [Электронный ресурс] // ISMS.online. URL: https://www.isms.online/nis-2/overview/digital-sovereignty/ (дата обращения: 11.12.2025).

4. The Rise of Digital Sovereignty: How Geopolitics Is Shaping Cybersecurity [Электронный ресурс] // LinkedIn Pulse. URL: https://www.linkedin.com/pulse/rise-digital-sovereignty-how-geopolitics-shaping-cybersecurity-fqu1c (дата обращения: 11.12.2025).

Александр Евгеньевич Бобер,
аспирант, Сибирский институт управления – филиал РАНХиГС,
E-mail: bober-ae@ranepa.ru

Alexander Evgenievich Bober,
Ph.D. Candidate, Siberian Institute of Management – branch of RANEPA,
E-mail: bober-ae@ranepa.ru

НАЦИОНАЛЬНАЯ ИНФОРМАЦИОННАЯ СЕТЬ ИРАНА: ЦИФРОВОЙ СУВЕРЕНИТЕТ КАК ИНСТРУМЕНТ ВНЕШНЕЙ ПОЛИТИКИ

IRAN'S NATIONAL INFORMATION NETWORK: DIGITAL SOVEREIGNTY AS A FOREIGN POLICY INSTRUMENT

Глобальные модели цифрового суверенитета: компаративный анализ. Цифровой суверенитет трансформировался из оборонительной концепции в комплексную геополитическую стратегию проецирования государственной власти в условиях формирования полицентричного миропорядка, катализируя процесс фрагментации глобального интернет-пространства («сплинтернет») как постепенного «переподключения» сетевой архитектуры с целью влияния на трансграничные потоки данных [10, с. 63-75]. Исламская Республика Иран реализует наиболее радикальную модель цифрового суверенитета через создание Национальной информационной сети (NIN) – альтернативной сетевой инфраструктуры как параллельного интернет-пространства [3, с. 1-2]. Кейс тринадцатидневного отключения глобального интернета в июне 2025 года, когда более 90 миллионов иранцев потеряли возможность выйти в глобальную сеть, продемонстрировал оперативную готовность NIN как инструмента внешнеполитического реагирования и трансформацию проекта в попытку восстановления государственного суверенитета через специфическую конфигурацию киберпространства [5, с. 1, 4].

Глобальный ландшафт цифрового суверенитета характеризуется формированием трех дистинктивных моделей: рыночно-ориентированная модель США, регуляционная модель Европейского союза и государственно-центричная модель Китая и России [8, с. 369-384]. Американская стратегия базируется на доминировании технологических корпораций, европейская – на нормативном регулировании через GDPR/DSA/DMA, китайско-российская – на государственном контроле и продвижении многосторонней модели интернет-управления с ключевой ролью государства в принятии решений [12, с. 8-11] [11, с. 16-18, 19-24, 28-30].

Иранская же модель представляет собой наиболее автаркическую форму цифровой суверенизации, выходящую за пределы создания национальных регуляторных режимов к построению альтернативной сетевой инфраструктуры как параллельного интернет-пространства [4, с. 1-3] [14, с. 1-2]. Позиционирование иранской модели в спектре глобальных стратегий выявляет её уникальность как предельного случая «жесткого» цифрового суверенитета, где контроль информационного пространства интегрирован во внешнеполитическую стратегию противодействия санкционному давлению и геополитической изоляции [13, с. 677-678].

Национальная информационная сеть: архитектура цифровой автономии. Техническая реализация иранской модели базируется на создании параллельной инфраструктуры. Концептуальная разработка Национальной информационной сети Ирана была инициирована в 2005 году как ответ на санкционное давление и киберугрозы со стороны западных государств, эволюционировав к комплексной стратегии цифровой автономии [17, с. 10-11, 19]. Принципиальное отличие иранской модели заключается в создании «скрытой сети» с маршрутизацией частных IP-адресов, доступной только внутри страны [4, с. 2].

Кейс тринадцатидневного отключения глобального интернета (13-25 июня 2025 года), связанный с эскалацией военного конфликта с Израилем, продемонстрировал техническую зрелость NIN как инструмента внешнеполитического реагирования [9, с. 40]. Операция «скрытого отключения» (stealth blackout) обеспечила снижение трафика к глобальному интернету на 90% при сохранении внутренних сервисов [9, с. 18-21], что свидетельствует о завершении трансформации из концептуального проекта в оперативную инфраструктуру цифровой автономии [9, с. 3-4].

Национальная информационная сеть как инструмент внешней политики. Техническая зрелость NIN, продемонстрированная в июне 2025 года, обеспечила её трансформацию в многофункциональный внешнеполитический инструмент. Она реализуется по трем направлениям: противодействие санкционному давлению, интеграция в ось цифрового суверенитета и использование киберпространства для прокси-стратегий. NIN реализует функцию противодействия санкциям через снижение уязвимости от отключения от критической цифровой инфраструктуры, оформляясь как механизм технологической автономии [5, с. 4].

Дипломатическое же измерение проявляется в продвижении концепции «многополярного киберпространства» через участие в разработке Конвенции ООН по киберпреступности [18, с. 1, 7]. Нельзя также не отметить процесс интеграции в ось Россия-Китай-Иран, который операционализируется через всеобъемлющее стратегическое

соглашение от 17 января 2025 года [1], предусматривающее обмен экспертизой в управлении национальными сегментами интернета и создание правил для технологических компаний [16; 6, с. 4]. Координация стратегий в киберпространстве отражает скоординированные политические меры в противодействии Западу, представляя из себя растущий вызов США [2]. Также Иран является полноправным членом Шанхайской организации сотрудничества (ШОС) с 2023 года и БРИКС с 2024 года. Это членство предоставляет Тегерану формальную платформу для участия в выработке коллективной позиции по вопросам цифрового управления. Исследования показывают, что ШОС и БРИКС систематически продвигают концепцию «киберсуверенитета» в противовес западной мультистейкхолдерной модели [16].

Таким образом, реализация NIN катализирует трансформацию глобальной архитектуры интернет-управления через легитимацию государственно-центричной модели [15, с. 15, 33-34], формирование альтернативных коалиций и углубление фрагментации интернет-пространства. Иранский опыт демонстрирует техническую реализуемость параллельного интернет-пространства, при этом потенциал экспорта модели создает мультипликативный эффект углубления «сплинтернета», а формирование оси Россия-Китай-Иран создает структурные основания для консолидации альтернативной модели цифрового миропорядка.

Структурные противоречия иранской модели. Несмотря на принципиальную реализуемость такой стратегии, практическая сторона реализации иранской модели цифрового суверенитета выявляет противоречие между внешнеполитическими задачами и внутриэкономическими издержками. Интернет-ограничения в период протестов 2022-2023 годов привели к падению трафика услуг передачи данных на 50% и существенным потерям прибылей операторов связи [7, с. 13]. Парадоксально, что инфраструктура, позиционируемая как стратегический актив, требует ценовых манипуляций для побуждения граждан к использованию: доступ к внутренним ресурсам предоставляется вдвое дешевле глобального интернета [7, с. 10-11]. Это структурная уязвимость Иранской модели, вынужденной балансировать между контролем и экономической эффективностью [7, с. 14-15].

Заключение. Проведённый анализ выявляет трансформацию NIN из инфраструктурного проекта в комплексный инструмент внешнеполитической стратегии, представляющий наиболее радикальную форму цифрового суверенитета. Июньское отключение 2025 года продемонстрировало техническую готовность сети как оперативного инструмента геополитического реагирования, однако структурные экономические противоречия ограничивают её долгосрочную устойчивость.

Геополитические последствия реализации NIN включают катализацию фрагментации глобального интернет-пространства, формирование альтернативных коалиций цифрового суверенитета и создание прецедента для экспорта модели. Иранский кейс демонстрирует предельный случай инструментализации цифровой инфраструктуры для внешнеполитических целей, где техническая реализуемость цифровой автономии сталкивается с экономическими издержками изоляции. В таких условиях актуальными предстают дальнейшие исследования адаптации модели в условиях технологических санкций и динамики социального сопротивления цифровой изоляции.

Список источников и литературы:

1. Договор о всеобъемлющем стратегическом партнёрстве между Российской Федерацией и Исламской Республикой Иран от 17 января 2025 г. [Электронный ресурс] // Официальный сайт Президента России. URL: http://kremlin.ru/supplement/6258 (дата обращения: 08.11.2025).

2. Al-Auqaili A. Russia-Iran-China Alliance Signals Deep Shift in Global Power / A. Al-Auqaili // Foreign Policy in Focus. — 2025. — 7 Aug. [Электронный ресурс]. URL: https://fpif.org/russia-iran-china-alliance-signals-deep-shift-in-global-power/ (дата обращения: 08.11.2025).

3. Anderson C. The Hidden Internet of Iran: Private Address Allocations on a National Network / C. Anderson // arXiv:1209.6398 [cs]. — arXiv, 2012. [Электронный ресурс]. URL: http://arxiv.org/abs/1209.6398 (дата обращения: 08.11.2025).

4. Aryan S. Internet Censorship in Iran: A First Look / S. Aryan, H. Aryan, J. A. Halderman // Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet. — Washington, DC : USENIX Association, 2013. [Электронный ресурс]. URL: https://www.usenix.org/system/files/conference/foci13/foci13-aryan.pdf (дата обращения: 08.11.2025).

5. Aryapour A. Iran's Stealth Internet Blackout: A New Model of Censorship / A. Aryapour // arXiv:2507.14183 [cs]. — arXiv, 2025. [Электронный ресурс]. URL: http://arxiv.org/abs/2507.14183 (дата обращения: 08.11.2025).

6. Azizi H. Strategic Transactionalism: The Iran-Russia Partnership / H. Azizi. — Doha : Middle East Council on Global Affairs, 2025. [Электронный ресурс]. URL: https://mecouncil.org/publication/strategic-transactionalism-the-iran-russia-partnership/ (дата обращения: 08.11.2025).

7. Conduit D. The political economy of digital authoritarianism: evidence from the Iranian regime's implementation of technology / D. Conduit // Democratization. — 2025. — Vol. 33, № 1. — P. 62-84. [Электронный ресурс]. URL:

https://www.tandfonline.com/doi/full/10.1080/13510347.2025.2514766 (дата обращения: 08.11.2025).

8. Floridi L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU / L. Floridi // Philosophy & Technology. — 2020. — Vol. 33, № 3. — P. 369-378. DOI: 10.1007/s13347-020-00423-6. [Электронный ресурс]. URL: https://link.springer.com/article/10.1007/s13347-020-00423-6 (дата обращения: 08.11.2025).

9. Iran's «Stealth Blackout»: A Multi-stakeholder Analysis of the June 2025 Internet Shutdown / Miaan Group, ASL19, IODA. — Atlanta : Miaan Group, 2025. [Электронный ресурс]. URL: https://miaan.org/report-on-irans-blackout-of-the-global-internet/ (дата обращения: 08.11.2025).

10. Mueller M. Will the Internet fragment? Sovereignty, globalization, and cyberspace / M. Mueller. — Cambridge, UK ; Malden, MA : Polity Press, 2017. — 177 p. — (Digital futures).

11. Nocetti J. A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union / J. Nocetti. — Paris : Ifri, 2024. — (Études de l'Ifri). [Электронный ресурс]. URL: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/ifri_nocetti_internet_fragmentation_february_2024.pdf (дата обращения: 08.11.2025).

12. Pohle J. Digital sovereignty / J. Pohle, T. Thiel // Internet Policy Review. — 2020. — Vol. 9, № 4. [Электронный ресурс]. URL: https://policyreview.info/concepts/digital-sovereignty (дата обращения: 21.10.2025).

13. Robles-Carrillo M. Sovereignty vs. Digital Sovereignty / M. Robles-Carrillo // Journal of Digital Technologies and Law. — 2023. — Vol. 1, № 3. — P. 673-690. DOI: 10.21202/jdtl.2023.29. [Электронный ресурс]. URL: https://www.lawjournal.digital/jour/article/view/236 (дата обращения: 08.11.2025).

14. The geopolitics behind the routes data travels: a case study of Iran / L. Salamatian, F. Douzet, K. Limonier, K. Salamatian // arXiv:1911.07723 [cs]. — arXiv, 2019. [Электронный ресурс]. URL: http://arxiv.org/abs/1911.07723 (дата обращения: 08.11.2025).

15. DeNardis L. The global war for internet governance / L. DeNardis. — New Haven : Yale University Press, 2014. — 296 p.

16. The New Authoritarian Axis: How Russia Multiplied Cooperation With China, Iran, and North Korea : Research & Analysis. — London : OpenMinds, 2025. [Электронный ресурс]. URL: https://www.openminds.ltd/reports/the-new-authoritarian-axis-how-russia-multiplied-cooperation-with-china-iran-and-north-korea (дата обращения: 08.11.2025).

17. Tightening the Net: Internet Security and Censorship in Iran. Part 1: The National Internet Project. — London : ARTICLE 19, 2016. — ISBN 978-1-910793-29-9. [Электронный ресурс]. URL: https://www.refworld.org/reference/countryrep/art19/2016/en/109598 (дата обращения: 08.11.2025).

18. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes : резолюция Генеральной Ассамблеи ООН 79/243 от 24 декабря 2024 г. — New York : UN, 2024. [Электронный ресурс]. URL: https://www.unodc.org/unodc/cybercrime/convention/home.html (дата обращения: 08.11.2025).

Головач Павел Николаевич,
студент юридического факультета Белорусского государственного университета, г. Минск, Республика Беларусь.
E-mail: pavelgolovac65@gmail.com

Научный руководитель:
Емельянович Ольга Викторовна,
доцент кафедры государственного управления юридического факультета Белорусского государственного университета, к.ю.н.
г. Минск, Республика Беларусь.
E-mail: emelyanovich@bsu.by

Golovach N. Pavel,
student of the Law Faculty of the Belarusian State University,
Minsk, Republic of Belarus.
E-mail: pavelgolovac65@gmail.com

Scientific supervisor:
Emelyanovich V. Olga,
Associate professor at the Chair of Public Administration, PhD in Law,
Faculty of Law, Belarusian State University, Minsk, Republic of Belarus.
E-mail: emelyanovich@bsu.by

СТРАТЕГИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЦИФРОВОГО СУВЕРЕНИТЕТА В РАМКАХ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ: СОВРЕМЕННЫЕ УГРОЗЫ И ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ

STRATEGIC BASIS FOR ENSURING INFORMATION SECURITY AND DIGITAL SOVEREIGNTY WITHIN THE COLLECTIVE SECURITY TREATY ORGANIZATION: CONTEMPORARY THREATS AND PERSPECTIVES FOR ENHANCEMENT

Аннотация. Исследование посвящено комплексному анализу стратегических и правовых основ обеспечения информационной безопасности в рамках Организации Договора о коллективной безопасности. На основе изучения ключевых документов организации выявляются системные проблемы, препятствующие формированию эффективной системы коллективной безопасности: фрагментарность правового поля, нормативные коллизии, декларативность норм и финансовые барьеры. Доказывается необходимость комплексной ревизии правовой базы и гармонизации национальных законодательств и создания действенной архитектуры коллективной информационной безопасности.

Ключевые слова. Информационная безопасность, цифровой суверенитет, ОДКБ, правовое регулирование, системные проблемы, киберпреступность, гармонизация законодательства, коллективная безопасность.

Abstract. The study is devoted to a comprehensive analysis of the strategic and legal basis for ensuring information security within the Collective Security Treaty Organization. Based on the examination of the Organization's key documents, systemic problems hindering the formation of an effective collective security system are identified: fragmentation of the legal framework, regulatory conflicts, declarative norms, and financial barriers. The study identifies the necessity of a comprehensive revision of a legal framework and harmonization of national legislations aimed at building an effective information security architecture.

Key words. Information security, digital sovereignty, CSTO, legal framework, systemic problems, cybercrime, harmonization of legislation, collective security.

Обеспечение информационной безопасности и цифрового суверенитета превратилось в стратегический элемент государственной политики на фоне стремительной трансформации характера угроз национальной и коллективной безопасности в XXI веке, что находит свое отражение как на национальном уровне, так и в рамках международных региональных организаций, к числу которых относится в том числе и Организация Договора о коллективной безопасности (далее – ОДКБ, Организация).

Договорно-правовая база ОДКБ в области информационной безопасности представляет собой многоуровневую систему, ядро которой образуют четыре системообразующих акта.

Соглашение о сотрудничестве в области обеспечения информационной безопасности от 30 ноября 2017 г (далее – Соглашение) [3]**.** Данный международный договор определяет конкретные механизмы сотрудничества. Его значимость заключается в детализации ключевых понятий в данной сфере и определении основных направлений взаимодействия. Преамбула Соглашения признает «необходимость соблюдения баланса между основными правами и свободами человека и эффективным противодействием угрозам», однако конкретные правовые гарантии и механизмы обеспечения такого баланса в тексте отсутствуют. Это создает риски произвольного толкования и принятия чрезмерных ограничительных мер на национальном уровне под предлогом обеспечения безопасности.

Статья 2 Соглашения вводит понятия: *«деструктивное информационное воздействие»*, *«информационная безопасность», «компьютерная атака», «угроза*

информационной безопасности», что создает единое понятийное поле для государств – членов ОДКБ. Статья 3 закрепляет перечень основных угроз и фокусирует усилия Сторон на противодействии конкретным вызовам. Статьи 4-8 детализируют направления сотрудничества (формирование практических механизмов совместного реагирования, развитие мер доверия и совершенствование технологической основы безопасности).

Ряд положений носят рамочный характер и требуют дальнейшей конкретизации. Например, ст. 6 обязывает Стороны «прилагать совместные усилия для выявления, предупреждения и нейтрализации угроз», однако механизм такого взаимодействия, порядок обмена оперативной информацией и принятия решений о совместных действиях не регламентированы.

Статья 15 Соглашения устанавливает, что Стороны «самостоятельно несут расходы», а вопрос о прочих расходах «решается в каждом отдельном случае». Подобная формулировка создает правовую неопределенность и может стать препятствием для финансирования масштабных совместных проектов или оперативного реагирования на конкретные угрозы.

Программа совместных действий по формированию системы информационной безопасности от 5 сентября 2008 г. (далее – Программа) [4]**.** Данный документ носит программный характер и заложил основу для последующего развития правовой базы. Программа определила первоначальный план действий в виде разработки понятийного аппарата, сравнительного анализа национальных законодательств и создание модели системы информационной безопасности. Именно в рамках данной Программы была предусмотрена разработка Соглашения.

Многие положения Программы выполнены или утратили свою значимость. Программа не актуализировалась, что создает правовую коллизию в области долгосрочного планирования. В разделе 1.1 упоминается «классификация угроз информационной безопасности», однако сама классификация так и не была разработана на уровне ОДКБ.

Стратегия коллективной безопасности ОДКБ на период до 2025 года (далее – Стратегия) [5]. Стратегия является документом высшего стратегического уровня, задающим общие ориентиры для всей деятельности Организации. В Стратегии информационная безопасность признана одним из ключевых направлений обеспечения коллективной безопасности (п. 6.5). Документ устанавливает стратегические цели: формирование системы информационной безопасности, развитие межгосударственного сотрудничества и выработка согласованных правил взаимодействия в информационной сфере.

Как и любой стратегический документ, Стратегия не содержит конкретных механизмов реализации. Пункт 6.5 ограничивается перечислением направлений деятельности, не детализируя их. Например, в документе практически не уделено внимания вопросам *защиты персональных данных*, что является критически важным элементом цифрового суверенитета в современную эпоху.

В отличие от национальных концепций (например, Концепции национальной безопасности Республики Беларусь [1]), в Стратегии ОДКБ отсутствует упоминание о необходимости обучения и повышения квалификации специалистов в области информационной безопасности на постоянной основе.

Протокол о взаимодействии по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г. (далее – Протокол) [2]. Рассматриваемый Протокол занимает особое место в договорно-правовой базе ОДКБ, поскольку он является первым и на сегодняшний день единственным специализированным актом, регламентирующим исключительно *оперативно-практическое взаимодействие компетентных органов* государств-членов в борьбе с киберпреступностью. Если Соглашение и Стратегия задают общие стратегические рамки, а Программа определяет общие программные цели, то Протокол уже фокусируется на процедурных и процессуальных аспектах сотрудничества.

Статья 1 Протокола содержит развернутые дефиниции ключевых терминов («информационная сфера», «преступление в сфере информационных технологий», «компьютерная информация» и «уполномоченный компетентный орган»). В отличие от других документов, носящих рамочный характер, Протокол имеет конкретный предмет регулирования – противодействие преступной деятельности. Статья 3 содержит перечень категорий преступлений, подпадающих под его действие (против основ конституционного строя, мира и безопасности человечества, собственно преступления в сфере ИТ). Важнейшим преимуществом Протокола является детальная регламентация процедуры взаимодействия (ст. 6, 7 Протокола). Статья 5 Протокола предусматривает исчерпывающий и практико-ориентированный перечень форм сотрудничества, включая не только традиционный обмен информацией, но и проведение скоординированных операций, создание совместных информационных систем, совместные научные исследования и, что особенно важно, *подготовку и повышение квалификации кадров*.

Однако эффективность протокола существенно ограничена привязкой к национальному уголовному законодательству и отсутствием унифицированных процессуальных норм. Также протокол не распространяется на гибридные угрозы, которые не всегда достигают порога уголовно наказуемого деяния, но при этом представляют

значительную опасность для информационной безопасности. Таким образом, он охватывает лишь отдельный аспект куда более широкого спектра угроз, описанных в Соглашении.

Проведенный анализ позволяет выявить ряд системных проблем, препятствующих формированию эффективной системы коллективной информационной безопасности в рамках ОДКБ:

1. Фрагментарность международно-правового регулирования. Договорно-правовая база ОДКБ в области информационной безопасности представляет собой совокупность разноуровневых актов, регулирующих различные аспекты информационной безопасности.

*2. Проблема гармонизации законодательств***.** Несмотря на провозглашенную в ст. 5 Соглашения цель по гармонизации национальных законодательств, государства-члены находятся на разных этапах цифровой трансформации и имеют различные подходы к регулированию киберпространства, защиты данных и противодействия дезинформации.

3. Финансовая неопределенность как системный барьер. Формулировка о том, что «Стороны самостоятельно несут расходы» создает системный финансовый барьер. Отсутствие четкого, предсказуемого механизма финансирования совместных проектов, операций по оперативному реагированию или создания информационной инфраструктуры делает их экономически необеспеченными.

4. Пробелы в регулировании новых вызовов и кадровом обеспечении. Правовая база ОДКБ демонстрирует системное отставание от динамики угроз. В ней отсутствует унифицированная классификация угроз информационной безопасности, а также стратегические положения о создании единого образовательного пространства и постоянной подготовке кадров в области информационной безопасности, что ставит под вопрос долгосрочную профессиональную состоятельность коллективной системы.

Заключение. Таким образом, исходя из всего вышесказанного, преодоление данных проблем требует не точечных изменений, а комплексной ревизии и кодификации правовой базы, гармонизации национальных законодательств и создания наднациональных имплементационных механизмов, обладающих реальными полномочиями и ресурсами.

Список источников и литературы:

1. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : решение Всебелорусского народного собрания Респ. Беларусь, 25 апр. 2024 г., № 5 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – URL: https://etalonline.by/document/?regnum=e01700001&q_id=0 (дата обращения: 10.10.2025).

2. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 23 декабря 2014 г. «Протокол о взаимодействии государств - членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере» [Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – URL: https://etalonline.by /document/?regnum=e01700001&q_id=0 (дата обращения: 10.10.2025).

3. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 30 ноября 2017 г. «О Соглашении о сотрудничестве государств – членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности» [Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – URL: https://etalonline.by /document/?regnum=e01700001&q_id=0 (дата обращения: 10.10.2025).

4. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 5 сентября 2008 г. № 05 «О Программе совместных действий по формированию системы информационной безопасности государств – членов ОДКБ» [Электронный ресурс] // Информационно-правовая система «Законодательство стран СНГ». – URL: https://base.spinform.ru/ show_doc.fwx?rgn=30848 (дата обращения: 10.10.2025).

5. Решение Совета коллективной безопасности Организации Договора о коллективной безопасности от 14 октября 2016 года «Об утверждении Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года» [Электронный ресурс] // Официальный сайт Организации Договора о коллективной безопасности. – URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do_/ (дата обращения: 10.10.2025).

Татьяна Александровна Гришанина,
Независимый исследователь,
E-mail: tatiana_grishanina@mail.ru

Tatiana A. Grishanina,
Independent researcher,
E-mail: tatiana_grishanina@mail.ru

ЦИФРОВАЯ СТРАТЕГИЯ ИЗРАИЛЯ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ НА БЛИЖНЕМ ВОСТОКЕ

DIGITAL STRATEGY OF ISRAEL IN THE MIDDLE EAST UNCERTAIN ENVIRONMENT

Аннотация. Автор исследует цифровую стратегию Израиля в контексте современных цифровых международных отношений, в частности во время текущего палестино-израильского конфликта на Ближнем Востоке. Цифровые международные отношения в регионе характеризуются высокой степенью неопределенности. Цель доклада – выявить особенности цифровой стратегии Израиля в условиях неопределенности на Ближнем Востоке. В докладе автор ставит вопрос о том, существует ли цифровой суверенитет Израиля. Исследование опирается на анализ правительственных документов Израиля в области цифровизации, данные Международного союза электросвязи по странам Ближнего Востока за 2023-2025 гг., а также отчеты международных аналитических центров США, Германии, Израиля, Эстонии о цифровой внешней политике Израиля. Результатом исследования является ряд общих выводов: регион характеризуется высокой степенью фрагментации киберпространства, цифровой разрыв на сегодняшний день практически непреодолим. Частные выводы касаются непосредственно цифровой стратегии Израиля: Израиль позиционирует себя в качестве государства, экспортирующего «цифровую революции» за счет сильной поддержки инновационных стартапов, Израиль включен в орбиту американской концепции «стран-единомышленников», одним из приоритетов является противодействие Ирану в киберпространстве, в частности в сфере кибертерроризма. С 2017 г. по 2025 г. цифровая стратегия Израиля претерпела значительные изменения: от открытости и инклюзии в сторону тотальной милитаризации.

Ключевые слова: цифровые международные отношения, цифровая внешняя политика, цифровая стратегия Израиля, цифровой разрыв, неопределенность, фрагментация, цифровой суверенитет.

Abstract. The author explores the digital strategy of Israel within the framework of digital international relations, narrowing the scope of research to the current Israeli-Palestinian conflict in the Middle East. Digital international relations in the region can be qualified as highly uncertain. The report aims at identifying the key directions of Israel's digital strategy. In the report, the author puts the research question, whether Israel is digitally sovereign. The research is based on the analysis of governmental documents on the digitalization of Israel, ICT Development Index in the Middle East 2023-2025 within the ITU Data Dashboard, international "think tank" reports of the USA, Germany, Israel, Estonia on Israel's digital foreign policy. The results of the research are divided into general and narrow. The general conclusions are the following – cyberspace of the region is highly fragmented, digital divide is almost irreversible. The narrow conclusions refer to the digital strategy of Israel, particularly, Israel has branded its digitalization in the international environment as the export of "digital revolution", Israel invests and attracts high investments to innovative startups, in cyberspace Israel acts within the framework of "like-minded states" established in the US National Security Strategy, one of the priorities of Israel's digital foreign policy is countering Iran in cyberspace which refers to cyberterrorism and malicious actions. The digital strategy of Israel has transformed from 2017 to 2025 from inclusion and openness to total militarization.

Key words: digital international relations, digital foreign policy, digital strategy of Israel, uncertainty, fragmentation, digital sovereignty.

Современные цифровые международные отношения характеризуются регионализацией, фрагментацией, неопределенностью, тенденциями к суверенизации киберпространства, выстраиванию цифровых границ, значительным усилением цифрового разрыва между сверхтехнологичными и слабо цифровизованными регионами. Данные проблемы со всей остротой проявляются в нестабильных, высококонфликтных подсистемах системы международных отношений. Доклад рассматривает частный случай проявления указанных выше тенденций на примере цифровой стратегии Израиля. Цель доклада — выявить особенности цифровой стратегии Израиля в условиях неопределенности на Ближнем Востоке на современном этапе. Методология исследования основывается на анализе правительственных документов Израиля, анализе статистических данных о цифровом развитии стран Ближнего Востока. Литературная база включает в себя работы современных российских и зарубежных исследователей в области цифровых международных отношений. Источниковая база состоит из резолюции ООН [1], правительственных документов Израиля в области цифровизации, отчетов международных аналитических центров США, Германии, Израиля, Эстонии о цифровой внешней политике

Израиля [2-12]. Результаты исследования имеют как теоретическую, так и практическую значимость и могут быть использованы в дальнейших исследованиях по проблеме цифровизации международных отношений.

Изучение литературы и источников по теме позволили автору выявить проблему в рамках заданной цели, а именно: обеспечение цифрового суверенитета при поддержке глобальной цифровой интеграции. В этом контексте возникает закономерный исследовательский вопрос: существует ли цифровой суверенитет Израиля? Чтобы ответить на этот вопрос, необходимо определить основные понятия, относящиеся к исследованию. Под фрагментацией киберпространства понимается процесс разделения Интернета на цивилизационные кластеры, национальные кластеры, социальные группы, культурные сообщества, которые создают собственные подсистемы глобального киберпространства. Неопределенность характеризуется таким состоянием цифровой системы, когда существует необходимость принятия решений в условиях ограниченной информации [13,14]. Цифровой суверенитет относится к категории государственного суверенитета, распространяющегося на киберпространство. В условиях технологического суверенитета государство проецирует власть на сферу развития технологий [15,16].

Индекс развития ИКТ — показатель, рассчитываемый Международным союзом электросвязи на основе ежегодного мониторинга данных о цифровом развитии государств — показывает, что в 2025 г. цифровые международные отношения характеризовались значительным цифровым разрывом в странах Глобального Юга. Эта проблема в частности особенно затрагивает регионы Африки и Ближнего Востока. Что касается стран Ближнего Востока, то «цифровой провал» в 2023-2025 гг. наблюдается в странах Леванта и Йемене. На наш взгляд, обострение палестино-израильского конфликта только усилило отставание (Рис. 1).

Рис. 1. Индекс развития ИКТ на Ближнем Востоке в 2023-2025 гг. [17].

Израиль занимает достаточно прочные позиции по индексу развития ИКТ, демонстрируя рост в среднем на 1% в год от 91,1% в 2023 г. до 92,5% в 2024 г. до 93,4% в 2025 г. Институционализация усилий по цифровой трансформация Израиля началась в 2017 г. с внедрением инициативы «Цифровой Израиль», положившей начало масштабной цифровой трансформации государственного аппарата Израиля [11]. Данная инициатива предусматривала всеобъемлющую программу цифровой трансформации, которая охватывала все стороны жизни населения, особое внимание уделяя сокращению разрыва между различными социальными слоями населения, стимулированию экономического роста, созданию «умного» правительства, взаимодействие с которым было бы интуитивно понятно гражданам. Считая Интернет общественным благом, Израиль предполагал на долгосрочной дистанции оказывать усиленную поддержку стартапам, привлекая иностранные инвестиции, создавать открытую и инклюзивную цифровую среду с целью общего демократического развития. Собственную цифровизацию Израиль позиционировал как «цифровую революцию» — ценность, которую государство могло бы экспортировать в качестве уникального продукта государства Израиль.

Цифровая трансформация Израиля осуществлялась в контексте общей напряженности на Ближнем Востоке. Однако, учитывая значительный цифровой разрыв с соседними арабскими странами, цифровая инициатива Израиля обладает серьезной

конкурентноспособностью. Тем не менее, несмотря на огромное экономическое, военное и политическое давление со стороны Израиля, у него появился прямой конкурент в области цифровой трансформации — Палестина, которая отличилась революционным нововведением в области защиты данных [18]. В 2021 г. в рамках создания цифрового правительства Палестина внедрила «принцип одного раза», который касается сбора данных пользователей. Согласно этому принципу, любые учреждения, государственные и негосударственные, могу собирать данные пользователей однократно. В течение 2021-2023 гг. этот принцип был внедрен в передовые практики Эстонии, Великобритании, Канады, Нидерландов; инициатива по принятию данного принципа всеми странами ЕС была выдвинута в 2023 г. Данный кейс демонстрирует, что страны с низким индексом цифровизации способны внедрять инновации, которые становятся драйверами мирового цифрового развития.

С 2022 г. Израиль уделяет особое внимание развитию национального генеративного искусственного интеллекта [9]. Цель национальной программы развития ИИ заключается в обеспечении глобального лидерства Израиля в этой сфере (Израиль занимает 9-е место в Глобальном индексе развития ИИ), поддержании высоких жизненных стандартов населения, стрессоусточивости в рамках национальной безопасности, стабильном экономическом росте. Такая стратегия определяется высоким уровнем концентрации талантливых кадров в сфере IT, высоким уровнем инвестиций в сектор ИИ, начиная с 2013 г., привлечением иностранных инвестиций. Новшеством последних лет стало стимулирование частных инвестиций, в том числе корпоративных инвестиций технологических гигантов Кремниевой долины. Так, Intel вкладывает от $2 млрд. до $25 млрд. в производство чипов, ИИ акселераторы, генеративные модели, в том числе обеспечивая развитие лабораторий в израильских университетах.

В 2023-2025 гг. ситуация серьезным образом изменилась, и Израилю приходится вкладывать средства в обеспечение цифровых границ, инвестировать в военные технологии для защиты собственного киберпространства [19-21]. Атаки со стороны Ирана сопровождаются массированным кибервоздействием. В июне 2025 г. иранские кибергруппы атаковали военную инфраструктуру Израиля, на что с его стороны последовал незамедлительный ответ. При этом иранские кибергруппы более децентрализованы и многочисленны, чем израильские, что указывает на высокую степень военной мобилизации израильского сегмента киберпространства [19]. Израиль закрывает цифровые границы для недружественных стран, оставляя возможность для сотрудничества в киберпространстве с США и странами ЕС.

Заключение. Таким образом, цифровая стратегия Израиля на современном этапе характеризуется следующими особенностями: переходом от инклюзии и открытости к полной милитаризации киберпространства с 2017 г. по 2025 г., приоритетом противодействия Ирану в киберпространстве (кибертерроризму, атакам на критическую инфраструктуру, нарративам военной пропаганды); преодолением «классового» цифрового разрыва внутри страны и цифрового разрыва с либеральными демократиями; включенностью в концепцию «стран-единомышленников» в Интернете; приоритетом поддержки инновационных стартапов; приоритетом развития облачных технологий, «умных» городов, 5G, цифровизации здравоохранения; привлечением государственных и частных американских инвестиций, обеспечением высокого уровня экспорта со странами ЕС. Все вышеизложенные особенности приводят к тому, что Израиль имплементирует кибернормы США и НАТО (Эстония). Это означает передачу части суверенитета в пользу стрессоустойчивости глобальной демократической цифровой системы.

Список источников и литературы:

1. Резолюция A/RES/ES-10/24 «Консультативное заключение Международного Суда относительно правовых последствий политики и действий Израиля на оккупированной палестинской территории, включая Восточный Иерусалим, и незаконности продолжающегося присутствия Израиля на оккупированной палестинской территории», принятая Генеральной Ассамблеей 18 сентября 2024 года [Электронный ресурс] // UNDOCS. URL: https://docs.un.org/ru/A/RES/ES-10/24 (дата обращения: 20.11.2025).

2. Axelrad, H. Sumkin, S. Haver, Ch. Promoting and Developing Israel Digital Transformation in Israel toward 2030 [Электронный ресурс] // Reichman University, Aaron Institute for Economic Policy in the Name of Aaron Dovrat z”l. Policy Paper 2022.03 / April 2022. URL: https://www.runi.ac.il/media/jk4di1sc/promoting-and-developing-digital-transformation-in-israel-toward-2030.pdf (дата обращения: 20.11.2025).

3. Ben, A. How Netanyahu Survives: Divide and Conquer in Gaza and at Home. // Foreign Affairs, November 10, 2025.

4. Efron, S. After the Guns Fall Silent in Gaza: The Tenuous Cease-Fire Between Israel and Hamas. // Foreign Affairs, October 10, 2025.

5. Export Strategy: Israel. ICT Sector Analysis for the Ministry of Foreign Affairs of the Republic of Estonia. Export Analysis and Strategy [Электронный ресурс] // The Ministry of Foreign Affairs of the Republic of Estonia, 2025. URL: https://vm.ee/sites/default/files/documents/2025-09/Israel%20ICT%20Report.pdf (дата обращения: 20.11.2025).

6. Israel Digital Economy. Israel Country Commercial Guide. U.S. Department of Commerce, International Trade Administration. 2025. 14 p. URL: https://www.trade.gov/country-commercial-guides/israel-digital-economy (дата обращения: 20.11.2025).

7. Israel Foreign Policy Index 2024: Findings of the Mitvim Institute Survey [Электронный ресурс] // Friedrich Ebert Stiftung, the Israeli Institute for Regional Foreign Policies, September 2024. URL: https://mitvim.org.il/wp-content/uploads/2024/09/Mitvim_Israeli-Foreign-Policy-Index-2024.pdf (дата обращения: 20.11.2025).

8. Israel / Palestinian Territories: Joint statement of the Ministers of Foreign Affairs - New York Call [Электронный ресурс] // MFA of Australia, July 29, 2025. URL: https://www.foreignminister.gov.au/minister/penny-wong/media-release/israel-palestinian-territories-joint-statement-ministers-foreign-affairs-new-york-call (дата обращения: 20.11.2025).

9. National Program for Artificial Intelligence. Israel Innovation Authority [Электронный ресурс] // Ministry of Innovation, Science and Technology, April, 2025. URL: https://innovationisrael.org.il/wp-content/uploads/2025/05/AI-National-Program-en-14.5.25.pdf (дата обращения: 20.11.2025).

10. Strategic Plan 2019-2021. The Government ICT Authority [Электронный ресурс] // Israel Digital Agency, 2019. URL: https://www.gov.il/BlobFolder/generalpage/strategic_plan_19/en/STRATIGY-%20ICT%20AUTHORITY%20-%20ENGLISH.pdf (дата обращения: 20.11.2025).

11. The Digital Israel National Initiative: The National Digital Program of the Government of Israel [Электронный ресурс] // Ministry for Social Equality of Israel, June 2017. URL: https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf (дата обращения: 20.11.2025).

12. The State of Israel's National Security. Doctrine and Policy Guidelines for 2025-2026 [Электронный ресурс] // The Institute of National Security Studies, Tel-Aviv University, 2025. URL: https://www.inss.org.il/publication/policy-2025/ (дата обращения: 20.11.2025).

13. Цветкова Н.А. Феномен цифровой дипломатии в международных отношениях и методология его изучения // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2020. № 2. С. 37–47.

14. Цветкова Н. А., Сытник А. Н., Гришанина Т. А. Цифровая дипломатия и digital international relations: вызовы и новые возможности // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 174–196.

15. Зиновьева Е.С, Булва В.И. Цифровой суверенитет Европейского Союза // Современная Европа. 2021. №2. С. 40-49.

16. Сучков М.А. «Геополитика технологий»: международные отношения в эпоху Четвертой промышленной революции // Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 138–157.

17. ICT Development Index. Middle East Countries, 2023-2025 [Электронный ресурс] // ITU Data Dashboard. URL: https://datahub.itu.int/dashboards/idi/?e=ISR&y=2025 (дата обращения: 20.11.2025).

18. Ibaid, M. Digital Government in the State of Palestine: Strategies and Recommendations. M-RCBG Associate Working Paper Series, No. 166 [Электронный ресурс] // Mossavar-Rahmani Center for Business and Government, Harvard Kennedy School, May 2021. URL: https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/Final_AWP_166.pdf (дата обращения: 20.11.2025).

19. Reddy, P. M. Part 1: The Iran-Israel Cyber Standoff - The Hacktivist Front [Электронный ресурс] // CloudSEK, June 19, 2025. URL: https://www.cloudsek.com/blog/part-1-the-iran-israel-cyber-standoff---the-hacktivist-front (дата обращения: 20.11.2025).

20. Shalom, Z. Israel's Foreign Policy – The Long Struggle Over Its Direction and Status. Book Review of "Knocking on Every Door – Israel's Foreign Policy, 1948-2018" by A. Ben-Zavi and G. Warsha. Institute for National Security Studies, Tel-Aviv University [Электронный ресурс] // URL: https://www.inss.org.il/strategic_assessment/israels-foreign-policy/ (дата обращения: 20.11.2025).

21. Zinovieva, E. Digital Geography and Digital Borders in the Era of Information Globalization. / Proceedings of Topical Issues in International Political Geography ed. by R. Bolgov, V. Atnashev, Yu. Gladkiy, A. Leete, A. Tsyb, S. Pogodin, A. Znamenski. Springer Geography, 2023. P. 145-151.

Юлия Искандеровна Джуматаева,
студент первого курса бакалавриата, факультет Международных отношений,
Дипломатическая академия МИД России,
E-mail: iskanderdzumataev@gmail.com

Julia I. Dzhumataeva,
first-year Bachelor's student in International Relations,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia,
E-mail: iskanderdzumataev@gmail.com

ЦИФРОВОЙ СУВЕРЕНИТЕТ И НАЦИОНАЛЬНЫЕ СТРАТЕГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DIGITAL SOVEREIGNTY AND NATIONAL INFORMATION SECURITY STRATEGIES

Аннотация. В статье рассматривается концепция «цифрового суверенитета» – способности государства сохранять независимость и защищать права граждан в цифровой среде. Эта концепция не имеет единого юридического определения, но на практике она реализуется через национальные стратегии, объединяющие технологическое развитие, законодательное регулирование и информационную безопасность. На примере России, Китая, ЕС и США показано, как разные подходы к цифровому суверенитету отражают политические и ценностные особенности каждой страны.

Ключевые слова: цифровой суверенитет, информационная безопасность, защита данных, кибербезопасность, национальная стратегия.

Abstract. The article examines the concept of "digital sovereignty" –the ability of a state to maintain independence and protect citizens' rights in the digital space. Without a unified legal definition, this concept is implemented through national strategies that combine technological development, legislative regulation, and information security. Using the examples of Russia, China, the EU, and the United States, the article demonstrates how different approaches to digital sovereignty reflect the political and value models of each country.

Key words: digital sovereignty, information security, data protection, cybersecurity, national strategy.

*Понятие «цифрового суверенитета»***.** Термин «цифровой суверенитет» не закреплен в официальных документах как юридическое понятие. Под суверенитетом обычно понимают независимость государства на международной арене и верховенство государственной власти внутри страны. Таким образом, цифровой суверенитет можно

определить как способность государства с помощью технологий и законов обеспечивать и защищать свою независимость, а также конституционные права граждан в информационном пространстве. Эта концепция стала особенно актуальной в связи с активным развитием информационно-коммуникационных технологий, начиная с 1990-х годов.

Следует отметить, что ни одно государство не может обладать полной цифровой независимостью. Для России одной из важных целей, закрепленных в законодательстве, является развитие информационных технологий и электронной промышленности, а также повышение эффективности организаций, занимающихся информационной безопасностью. Эти задачи соответствуют идее цифрового суверенитета и стали особенно важными в условиях санкционного давления.

Цифровой суверенитет тесно связан с информационной безопасностью. Информационная безопасность определяется как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз. Она обеспечивает конституционные права и свободы граждан, суверенитет, территориальную целостность и устойчивое развитие страны. Это означает, что без информационной безопасности невозможно достичь цифрового суверенитета.

Национальная стратегия обеспечения информационной безопасности России. Среди приоритетов – защита информации от влияния иностранных государств на информационное пространство России, противодействие распространению недостоверной информации, а также борьба с киберпреступностью, включая мошенничество и хакерские атаки. Кроме того, важной задачей является обеспечение безопасности инфраструктуры, что подразумевает сокращение зависимости от импортных технологий и их замену отечественными аналогами. Это касается разработки российского программного обеспечения и использования местных компонентов в производстве. Стремление отказаться от иностранных ИТ-решений также связано с рисками утечки персональных данных, что особенно опасно для критической информационной инфраструктуры.

Национальная стратегия обеспечения информационной безопасности других государств. Китай реализует концепцию цифрового суверенитета через строгое регулирование киберпространства в пределах национальных границ. Основой этого подхода является Закон о кибербезопасности 2017 года, который закрепляет контроль государства над информационной инфраструктурой, обязывает компании хранить данные на территории КНР и предоставлять доступ к ним уполномоченным органам. Для ограничения влияния иностранных технологий Китай блокирует такие платформы, как

Google и Facebook[5], одновременно развивая национальные аналоги, например Baidu и WeChat. Кибербезопасность в Китае курируется несколькими государственными структурами, включая Министерство промышленности и информатизации и Государственную канцелярию интернет-информации. Несмотря на меры контроля, китайские компании, как и другие участники глобального цифрового пространства, подвержены кибератакам, что показал инцидент с банком ICBC в 2023 году.

В основе цифрового суверенитета Европейского союза лежит защита прав граждан и их персональных данных. Это было закреплено в Общем регламенте о защите данных (GDPR), который с 2018 года установил высокие стандарты в этой области. Параллельно ЕС развивает собственную технологическую экосистему, чтобы снизить зависимость от неевропейских корпораций. Стратегии, такие как «Формирование цифрового будущего Европы», поддерживают создание локальных инфраструктурных проектов, включая облачную платформу Gaia-X. Для укрепления кибербезопасности в 2023 году была введена директива NIS2. Она ужесточает требования для критических секторов экономики и цифровых сервисов, обязывая их внедрять модели управления киберрисками, проводить оценку цепочек поставок и создавать системы оперативного оповещения об инцидентах. Страны-члены ЕС должны интегрировать эти положения в национальные законы до октября 2024 года, однако к середине года эту задачу выполнили лишь немногие государства, включая Норвегию и Францию.

Подход США к цифровому суверенитету изначально основывался на принципах свободы интернета и минимального вмешательства государства. Однако в последние годы акцент сместился в сторону защиты национальной безопасности и критической инфраструктуры. Знаковым документом стал CLOUD Act (2018), который предоставил американским правоохранительным органам расширенные полномочия по доступу к данным граждан, даже если они хранятся за пределами США. Дальнейшее ужесточение регулирования продолжилось с принятием в 2021 году Указа № 14028 «Об усилении кибербезопасности страны». Этот документ установил строгие требования к безопасности программного обеспечения, поставляемого для государственных нужд. Ключевым нововведением стала обязательная спецификация программных компонентов –подробный перечень всех библиотек и модулей, используемых в продукте. Без этой спецификации государственные органы не могут закупать программное обеспечение. Несмотря на усиление регулирования, на практике многие компании сталкиваются с трудностями в обеспечении кибербезопасности. Согласно исследованию 2024 года, крупные обновления

[5] Принадлежит компании Meta, запрещена и признана экстремисткой организацией на территории России.

программного обеспечения проходят полный аудит безопасности только в половине случаев, что свидетельствует о сохраняющихся пробелах в защите цепочек поставок ПО.

Заключение. Понятие «цифровой суверенитет», не имея единого юридического определения, на практике понимается как способность государства обеспечивать свою независимость и защищать конституционные права граждан в цифровом пространстве. Анализ подходов различных стран показывает, что, несмотря на общую цель – укрепление национальной безопасности и технологической самостоятельности, – методы её достижения значительно различаются, отражая разные политические и ценностные модели.

Россия делает акцент на защите своего информационного пространства от внешнего влияния и ускоренном импортозамещении, особенно в условиях санкционного давления. Китай реализует модель жесткого государственного контроля над инфраструктурой и данными, сочетая изоляцию иностранных платформ с развитием национальных аналогов. Европейский союз строит свой цифровой суверенитет вокруг защиты персональных данных граждан и создания собственных технологических экосистем, делая ставку на нормативное регулирование и кибербезопасность. США, исторически отстаивавшие свободу интернета, в последние годы сместились в сторону усиления контроля для защиты национальной безопасности, что выразилось в законах, расширяющих доступ спецслужб к данным и ужесточающих требования к безопасности ПО для государственного сектора.

Список источников и литературы:

1. Володенков С.В. Феномен цифрового суверенитета современного государства в условиях глобальных технологических трансформаций: содержание и особенности // Журнал политических исследований. 2020. № 4. С. 3–11.

2. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

3. Ефремов А.А. Формирование концепции информационного суверенитета государства // Право: Журнал Высшей школы экономики. 2017. № 1. С. 201–215.

4. Зинченко С.А. Деятельность социальных сетей по распространению экстремизма: кейс Meta[6] // Социальные и психологические проблемы глазами молодых – 2022: сборник материалов XXVI Междунар. научно-практич. конф. студентов, аспирантов и молодых ученых. Сыктывкар, 2022. С. 178–180.

5. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

[6] Компания Meta запрещена и признана экстремисткой организацией на территории России.

Иванов Евгений Олегович,
соискатель кафедры мировых политических
процессов МГИМО (У) МИД России,
eugene4712@mail.ru

Evgeniy O. Ivanov,
Postgraduate researcher, Department of World Politics,
MGIMO University,
eugene4712@mail.ru

СОТРУДНИЧЕСТВО ГОСУДАРСТВ ЛАТИНСКОЙ АМЕРИКИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИКТ В РАМКАХ ОАГ

COOPERATION OF THE LATIN AMERICAN STATES IN THE AREA OF ICT SECURITY WITHIN THE OAS

Аннотация. Основным форматом взаимодействия в области обеспечения международной информационной безопасности (далее − МИБ) в Латинской Америке является Организация американских государств (далее − ОАГ). Благодаря доктринальным документам и значительному институциональному инструментарию она позволяет государствам региона наращивать потенциал и обмениваться опытом по вопросам противодействия использованию ИКТ в террористических и преступных целях, а также имплементировать меры по укреплению доверия в цифровой среде. Вместе с тем, в силу доминирующего положения США организация испытывает ряд ограничений.

Ключевые слова: международная информационная безопасность, Организация американских государств, цифровая среда, меры по укреплению доверия, США, Бразилия, Аргентина.

Abstract. The basic format of cooperation on international information security in Latin America is the Organization of American States (OAS). Due to its doctrinal documents and significant institutional instruments, it lets the states of the region build capacities and exchange experience in the field of combatting using ICT for terrorist and criminal purposes, as well as implement confidence-building measures in the digital environment. However, due to the US dominant position, the organization has some limitations.

Keywords: international information security, Organization of American States, digital environment, confidence-building measures, USA, Brazil, Argentina.

Доктринальные документы. Сотрудничество в обеспечении МИБ в рамках ОАГ имеет достаточно большую нормативно-правовую базу. Ещё в 2004 году была принята Межамериканская стратегия по борьбе с угрозами кибербезопасности, где в качестве приоритетных сфер взаимодействия были указаны защита критической инфраструктуры, безопасность данных и гарантии прав человека на неприкосновенность частной жизни в цифровой среде. Среди основных угроз, в свою очередь, выделены использование ИКТ в террористических и преступных целях [3].

Другим важным документом является резолюция об укреплении безопасности ИКТ и противодействии терроризму в Западном полушарии, принятая в феврале 2016 года на пятом пленарном заседании Межамериканского комитета по борьбе с терроризмом (Comité Interamericano contra el Terrorismo, CICTE). Среди основных целей документа обозначены повышение стабильности, предсказуемости, открытости и безопасности в цифровой среде, а также создание групп по реагированию на компьютерные инциденты (Computer Security Incident Response Team, CSIRT) в целях превращения Интернета в мирную и безопасную среду [10].

Стоит также отметить, что именно CICTE является основным форматом взаимодействия государств-членов ОАГ в сфере обеспечения МИБ, так как на него возложена задача по формированию системы наблюдения, предупреждения и реагирования на инциденты в области безопасности ИКТ в рамках организации.

Другие форматы сотрудничества. Важную роль в обеспечении информационной безопасности в Западном полушарии играет и процесс REMJA, представляющий собой встречи генеральных прокуроров и министров юстиции государств-членов ОАГ. Его достижением является налаживание сотрудничества законодательных органов в сфере борьбы с ИКТ-преступностью и программы по повышению квалификации прокуроров и судей в сфере безопасности ИКТ [1, с. 39-40].

Первое упоминание преступлений в сфере компьютерной информации относится ко второму заседанию REMJA, прошедшему ещё в марте 1999 года. Тогда было рекомендовано создание межправительственной экспертной группы, которая должна проанализировать и оценить существующие и потенциальные вызовы безопасности ИКТ в Западном полушарии, и нормативно-правовые акты, нацеленные на противодействие злоумышленникам [6].

Кроме того, процесс REMJA занимается внерегиональным сотрудничеством в борьбе с ИКТ-преступностью, в частности, с ООН, ЕС, АТЭС, ОЭСР, Британским Содружеством и Интерполом [4], а также проводит семинары по сбору электронных

доказательств и совершенствованию правовых и технических возможностей противодействия преступлениям в сфере компьютерной информации [5].

Внимание МИБ уделяет и Межамериканский банк развития (далее − МАБР). В 2022 году он опубликовал тематический доклад, в котором отмечался рост преступлений с использованием ИКТ в связи с пандемией COVID-19. Кроме того, его авторы подчеркнули «фрагментированную и поляризованную глобальную архитектуру» обеспечения МИБ, но возложили вину за её текущее состояние на тех, кто пытается достичь «цифрового суверенитета» и «стратегической автономии» [2]. Ещё одним столпом обеспечения МИБ в Западном полушарии является Рабочая группа по сотрудничеству и укреплению доверия в цифровой среде, учреждённая в 2017 году по инициативе CICTE. Группа уделяет внимание проведению конференций и семинаров, созданию дискуссионных площадок между странами, входящими в ОАГ, а также компьютерным инцидентам и обмену информацией о них. Особый акцент делается на том, что данные меры носят лишь добровольный, а значит, юридически необязательный характер [9].

Ограничения. Тем не менее, несмотря на институционализацию сотрудничества и практические достижения, взаимодействие в рамках ОАГ подвержено ряду проблем, главной из которых является разное понимание угроз безопасности ИКТ. В силу доминирующего подхода США, желающих сохранить свободу для манёвра, организация не занимается военно-политическими угрозами МИБ и не отстаивает идею сугубо мирного использования ИКТ государствами. В то же время, для многих стран Латинской Америки, в том числе Бразилии [8] и Аргентины [7], эти положения крайне важны, так как значительная часть государств региона придерживается принципов уважения суверенитета, невмешательства во внутренние дела и мирного разрешения споров, что влияет и на их подходы к обеспечению МИБ.

Заключение. Можно констатировать, что ОАГ является важным форматом взаимодействия государств Латинской Америки в сфере обеспечения МИБ, так как располагает значительным институциональным инструментарием. Вместе с тем, по причине доминирующего положения США организация охватывает далеко не весь спектр угроз безопасности ИКТ, оставляя «за скобками» их применение в военно-политических целях, противоречащих общепризнанным принципам международного права, а также рассматривает меры по укреплению доверия в цифровой среде как «вещь в себе», не помещая её в контекст необходимости сугубо мирного использования ИКТ и декларируя их добровольный характер.

При этом, в плане противодействия террористическим и криминальным угрозам ОАГ наработала солидную правовую и техническую базу, что делает этот формат

привлекательным для латиноамериканских стран, но сотрудничество в рамках организации воспринимается ими как «необходимое, но не достаточное».

Список источников и литературы:

1. Ерёмин А.А. Организация американских государств и региональная безопасность. М., 2020, Издательство «Аспект Пресс», 176 с.
2. Amenazas de ciberseguridad: implicaciones para América Latina y el Caribe. *Revista Seguridad 360*. El 14 de julio de 2022. Available at: https://revistaseguridad360.com/noticias/amenazas-en-ciberseguridad/ (accessed 28.10.2025).
3. Comprehensive Inter-American Cybersecurity Strategy. *Organization of American States*. June 8, 2004. Available at: https://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm (accessed 28.10.2025).
4. Conclusions and Recommendations of REMJA-VI. *Organization of American States*. August 4, 2006. Available at: https://www.oas.org/juridico/english/moj_vi_recom_en.pdf (accessed 28.10.2025).
5. Conclusions and Recommendations of REMJA-X. *Organization of American States*. October 16, 2015. Available at: https://www.oas.org/en/sla/dlc/remja/pdf/remja_x_rec_conc_en.pdf (accessed 28.10.2025).
6. Conclusions and Recommendations of the Second Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas. *Organization of American States*. March 3, 1999. Available at: https://www.oas.org/juridico/english/remjaII_recom.pdf (accessed 28.10.2025).
7. Estrategia Nacional de Ciberseguridad de la República Argentina. *El Gobierno de Argentina*. El 14 de julio de 2023. Available at: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904 (accessed 28.10.2025).
8. Estratégia Nacional de Segurança Cibernética. *Presidência da República*. De 5 de fevereiro de 2020. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm (accessed 26.10.2025).
9. IV Reunión del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio. *Organización de Estados Americanos*. El 26 de octubre de 2022. Available at: https://www.oas.org/ext/es/principal/calendario/evento/id/63 (accessed 26.10.2025).
10. Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas. *U.S. Department of State*. February 26, 2016. Available at: https://2009-2017.state.gov/p/wha/rls/259346.htm (accessed 26.10.2025).

Эмин Эльчинович Мирзоев,
студент 2 курса бакалавриата,
Тюменского государственного университета
Направление: «Международные отношения: глобальные тренды взаимодействия»
E-mail: stud0000304266@utmn.ru

Emin E. Mirzoev,
second year of the bachelor's degree student,
Tyumen State University
Major: «International relations: global trends of interaction»
E-mail: stud0000304266@utmn.ru

ИНФОРМАЦИОННОЕ ПРОТИВОСТОЯНИЕ В АТР: ПОЛИТИЧЕСКИЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТЫ ФОРМИРОВАНИЯ НОВОЙ РЕАЛЬНОСТИ

INFORMATION CONFRONTATION IN ATR: POLITICAL TECHNOLOGIES AS TOOLS FOR SHAPING A NEW REALITY

Аннотация. В статье анализируются изменения в информационном ландшафте Азиатско-Тихоокеанского региона (АТР) после приостановки программ USAID в январе 2025 г. Рассматриваются новые политические технологии региона: примеры «войн памяти», фреймирования и сетевых движений. Предлагаются методы противодействия для укрепления информационной устойчивости региона в условиях глобальной цифровизации.

Ключевые слова: Дезинформация, Азиатско-Тихоокеанский регион, QUAD, AUKUS, психологические операции, войны памяти, нарратив жертвы, Milk Tea Alliance.

Abstract. The article analyzes changes in the information landscape of the Asia-Pacific (AP) region after the suspension of USAID programs in January 2025. Through new political technologies of the region: examples of "memory wars", framing and network movements are considered. Countermeasures are proposed to strengthen the region's information resilience in the context of global digitalization.

Key words: Disinformation, Asia-Pacific region, QUAD, AUKUS, psychological operations, memory wars, victim narrative, Milk Tea Alliance.

Информационный фон Азиатско-Тихоокеанского региона. Современный Азиатско-Тихоокеанский регион (АТР) представляет собой плацдарм глобального информационного противостояния, где политические технологии активно формируют новую международную реальность.

Структурные изменения в архитектуре медиавлияния, выразившиеся в свертывании ряда традиционных программ финансирования, создали условия для трансформации методов воздействия. На смену прежним инструментам приходят сложные формы когнитивного влияния, включая целенаправленное переписывание исторических нарративов, манипулятивное фреймирование и координацию децентрализованных сетевых движений. В этой новой реальности успех обеспечения информационного суверенитета стран региона напрямую зависит от выработки комплексного ответа, сочетающего развитие собственных медиаресурсов, международное сотрудничество и подготовку специалистов для эффективного противодействия вызовам цифровой эпохи.

Агенты влияния в АТР. Формирование новой информационной реальности в АТР происходит при активном участии широкого спектра акторов, чье влияние можно систематизировать в соответствии с классической концепцией видов власти: по аналогии с концепциями «острой силы», «умной силы» и «мягкой силы», которые в своих работах описывали Джозеф Най и Уолтер Рассел.

1. Военно-политические альянсы. Военно-политические альянсы, так или иначе аффилированные с США, являются QUAD (Quadrilateral Security Dialogue. Участники: Индия, Япония, США и Австралия), а также AUKUS (акроним из названия стран-участниц альянса. Участники: Australia, United Kingdom, United States). Альянсы важны как часть общего давления в АТР, которое только нарастает. Мы можем напрямую увидеть, например, по переброску американских частей из Восточной Европы в Индо-Тихоокеанский регион [2].

2. Информационные агенты влияния. США имеет ряд новостных сайтов и аналитических ведомств. Некоторые из них, в связи с закрытием USAID либо приостановили свою деятельность, либо полностью закрылись. Та часть новостных сайтов, что работает, имеет слишком малое количество просмотров, чтобы формировать общественное мнение хоть в каком-то серьёзном объёме. Можно сказать, что оставшиеся источники СМИ созданы для «внутреннего потребителя» – англоговорящие читатели, заинтересованные в новостях АТР.

3. Психологические операции. Особенно актуальны на данный момент. В условиях, когда государства всё чаще задумываются над суверенными СМИ и сохранением единого цифрового пространства, традиционные СМИ теряют свою актуальность, в отличие от отдельных акторов и общественных движений, которые они создают.

Актуальные политические технологии в АТР. За последние несколько лет можно вспомнить ряд операций, проводимых в АТР.

1. Проведение «Войн памяти». Для региона характерно проведение «войн памяти». Политика, опробованная в Восточной Европе в той или иной степени, ныне практикуется в АТР.

В августе 2025 г. священнослужители на Тайване отслужили панихиду по группе японских солдат времён Второй мировой. На мероприятие свою речь соболезнования отправил Такамара Фукуока – японский министр здравоохранения, труда и социального обеспечения. Вся эта церемония была практически показательно проведена перед 80-летием празднования Китаем в честь окончания Второй мировой войны [4].

2. Нарратив жертвы и фреймирование. Для АТР нарратив жертвы характерен также, как и для всего мира. После Второй мировой войны идея о том, что небольшие и слабые сообщества априори не могут ошибаться и всегда находятся в состоянии жертвы актуальны и будут оставаться таковыми ещё долго.

Как пример – религиозная секта «Церковь Сиона», функционирующая в Пекине, Гонконге и других крупных китайских городах. Постепенно из-за некоторых высказываний, нетрадиционных практик и чёрной бухгалтерии отделения церкви были закрыты, а секта была запрещена. После этого СМИ стали озвучивать нарратив: «Китай воюет со всех христианским миром» по аналогии с тибетским и уйгурским притеснениями в прошлом [3].

3. Сетевые движения. Актуальными для региона являются сетевые движения. Феномен «Clicktivism-a» в эпоху всеобщей цифровизации становится всё более и более актуальным.

Главным таким объединением сетевых оппозиционеров в Азии на данный момент является «Milk Tea Alliance». Возникшее как интернет-мем, организация постепенно переросла в крупное сетевое движение, объединяющее протесты в Китае, Таиланде, Индии, Мьянме и других странах. В данном контексте напиток, в честь которого назван альянс – интернациональный чай с молоком и различные его вариации, популярен во многих странах Азии и подчёркивает общую идею борьбы за демократию по всему АТР [1].

Подводя итог, можно сказать, что несмотря на смену администрации президента США, общий нарратив в АТР остаётся таким же. Главная проблема в том, что СМИ теперь не выстраиваются в стройную, ровную повестку, уже нельзя отследить инициатора той или иной провокации.

Методы противодействия. В условиях усиления психологических операций и ослабления традиционных каналов влияния, необходим многоуровневый, системный подход.

1. Международное сотрудничество. Странам АТР не следует «закрываться» в рамках своей страны или одного региона. Современные страны должны понять, что создание контр-нарративов не просто возможно, а желаемо. Существует потребность в создании общей дискурсной рамки, которая могла бы поспособствовать созданию единого информационного пространства.

2. Системный подход к подбору кадров. Государствам АТР необходимо задуматься о подготовке квалифицированных кадров – специалисты в кибербезопасности, ведению когнитивных войн, специалисты по рекламе и связям с общественностью.

3. Контроперации и создание привлекательного образа страны. Пожалуй, это является основным и самым важным. Необходимо задумываться над созданием контрнарративов как внутри своей страны, так и за рубежом.

Заключение. В АТР политические технологии остаются мощным инструментом геополитического влияния, особенно в условиях перераспределения сил. Ослабление традиционных каналов влияния открывает окно для региональных государств в укреплении суверенитета над информационным пространством. В будущем ожидается дальнейшая поляризация: с одной стороны, рост информационных угроз, с другой – консолидация АТР вокруг общих ценностей.

Список источников и литературы:

1. Benkitni A., Forehand J. A. *The Milk Tea Alliance as Internationalizing Protest* [Электронный ресурс] // *Journal of Politics and Governance.* – 2025. – Т. 15, № 3. – С. 16–31. URL: https://so03.tci-thaijo.org/index.php/jopag/article/view/279171 (дата обращения: 05.11.2025).

2. Cook L., McGrath S. The U.S. draws down troops on NATO's eastern flank as Europe frets about a security vacuum [Электронный ресурс] // The New York Times. – 2025. – 29 окт. URL: https://www.nytimes.com/2025/10/29/world/europe/us-troops-eastern-europe-romania.html?ysclid=mhg24sm7e4143214957 (дата обращения: 05.11.2025).

3. Fu B. China's War on Christians [Электронный ресурс] // Tablet Magazine. – 29 окт. 2025. URL: https://www.tabletmag.com/sections/news/articles/china-war-christians-zion-church?utm_source=chatgpt.com (дата обращения: 05.11.2025).

4. 屏東潮音寺弔念二戰死難者 – 日官員首度致詞 [Электронный ресурс] // 中央社 (CNA). 2025, Aug 3. URL: https://www.cna.com.tw/news/aloc/202508030178.aspx (дата обращения: 05.11.2025).

Алексей Вячеславович Ордин,
докторант Московского авиационного института (государственного технического университета), магистр международных отношений,
магистр права, к.т.н., эксперт в области цифровой дипломатии и международной кибербезопасности,
E-mail: Alexey_ordin@mail.ru

Alexey V. Ordin,
Doctoral Candidate, Moscow Aviation Institute (National Research University),
Master of International Relations,
Master of Law, Ph.D. in Engineering, expert in digital diplomacy and international cybersecurity,
E-mail: Alexey_ordin@mail.ru

НОВЫЕ РУБЕЖИ МЕЖДУНАРОДНОЙ СЕРТИФИКАЦИИ И ДОВЕРИЯ В КИБЕРБЕЗОПАСНОСТИ: ОПЫТ CREST И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ NGFW-ТЕХНОЛОГИЙ

NEW FRONTIERS OF INTERNATIONAL CERTIFICATION AND TRUST IN CYBERSECURITY: CREST EXPERIENCE AND PROSPECTS FOR NGFW TECHNOLOGIES

Аннотация. В работе рассматриваются современные тенденции международной сертификации в области кибербезопасности, особенности применения подходов CREST (Council of Registered Ethical Security Testers) и роль технологий NGFW (Next Generation Firewall) в формировании доверенной цифровой среды. Анализируется взаимосвязь между технологическим развитием и политико-правовыми механизмами обеспечения цифрового суверенитета.

Ключевые слова: NGFW, CREST, международная сертификация, кибербезопасность, цифровой суверенитет, кибердипломатия.

Abstract. The article examines current trends in international cybersecurity certification, the specific features of applying the CREST framework, and the role of Next Generation Firewall technologies in shaping a trusted digital environment. The study analyzes the relationship between technological development and the political-legal mechanisms used to ensure digital sovereignty.

Key words: NGFW, CREST, international certification, cybersecurity, digital sovereignty, cyber diplomacy.

Современные вызовы доверия в киберпространстве. В условиях стремительного роста трансграничных цифровых угроз особую значимость приобретает формирование устойчивых механизмов международного доверия к инфраструктуре кибербезопасности [7]. Государства сталкиваются с необходимостью согласования подходов к управлению

рисками, обеспечения технологической прозрачности и выработки универсальных инструментов атрибуции киберинцидентов [3]. По мере усложнения методов воздействия на информационные системы доверие трансформируется из сугубо технической категории в политико-правовой феномен, определяющий возможности трансграничного обмена данными, взаимного признания результатов аудита и сертификации, а также институциональной совместимости цифровых экосистем [1].

NGFW как инструмент гибридной киберзащиты. Технологии межсетевого экранирования нового поколения эволюционировали от базовой фильтрации сетевого трафика к комплексным системам обнаружения и предотвращения угроз, использующим методы машинного обучения, анализ контекста и поведенческие модели [5]. NGFW обеспечивает не только контроль сетевых потоков, но и формирование доверенной цифровой среды, инвентаризацию активов и интеграцию с национальными центрами мониторинга и реагирования (SOC, CERT) [6].

Современные NGFW-системы выполняют функции, недоступные традиционным средствам защиты: корреляцию многовекторных атак, управление уязвимостями в режиме реального времени и оркестрацию процессов реагирования. В результате NGFW становится ключевым элементом архитектуры цифрового суверенитета, формируя масштабируемый и согласованный защитный контур государственного и корпоративного секторов [5].

Обоснование выбора NGFW и CREST. Выбор NGFW и стандарта CREST в качестве ключевых кейсов обусловлен тем, что именно они отражают актуальные потребности государств ЕАЭС в формировании доверенной цифровой среды и гармонизации подходов к обеспечению кибербезопасности. NGFW представляет собой зрелую технологическую платформу, позволяющую выстраивать сопоставимые требования к защищённости информационных систем, обеспечивать совместимость национальных систем мониторинга и повышать устойчивость критической инфраструктуры.

CREST выбран как пример международной сертификации, демонстрирующий практико-ориентированную модель профессионального признания и унификации экспертных компетенций. В отличие от формальных нормативных стандартов, CREST обеспечивает аккредитацию специалистов, стандартизированные процедуры тестирования на проникновение и высокий уровень транспарентности результатов оценки безопасности [2].

CREST как международный стандарт. Международная организация CREST разработала унифицированную модель аккредитации специалистов и компаний, обеспечивающую высокие требования к качеству тестирования на проникновение, реагирования на инциденты и аудита информационной безопасности. CREST-подход

формирует профессиональное сообщество, основанное на проверяемых компетенциях, строгих этических принципах и институциональной прозрачности. Это способствует интернационализации услуг по оценке безопасности и формированию инфраструктуры доверия между государственными структурами, частным сектором и международными организациями [2].

Перспективы адаптации CREST-подхода в ЕАЭС. В условиях евразийской экономической интеграции актуализируется необходимость создания общей системы аккредитации экспертов в области кибербезопасности. Адаптация CREST-подхода может способствовать повышению качества национальных процессов аудита, обеспечению сопоставимости требований государств-членов ЕАЭС, сокращению издержек бизнеса и формированию общего рынка кибербезопасностных услуг. Такой механизм будет способствовать укреплению трансграничного доверия при сохранении национального контроля над критически значимой инфраструктурой.

Роль цифровой дипломатии. Цифровая дипломатия становится связующим звеном между технологическими разработчиками, регуляторами и международными институтами. Цифровые атташе обеспечивают продвижение национальных технологических интересов, формирование диалога между государствами, научным сообществом и бизнесом, а также развитие международных партнёрств. В результате цифровая дипломатия интегрирует технические и политико-правовые элементы международной кибербезопасности.

Заключение. Развитие международных механизмов доверия в киберпространстве требует комплексного подхода, сочетающего внедрение передовых технологических решений, развитие профессиональных стандартов и активное использование дипломатических инструментов. Для государств ЕАЭС адаптация CREST-подхода и внедрение NGFW-технологий может стать важным шагом в укреплении цифрового суверенитета, обеспечении сопоставимости национальных стандартов и интеграции в глобальные механизмы доверия в сфере кибербезопасности.

Список источников и литературы:

1. Документы цифровой повестки Евразийского экономического союза (Цифровая повестка ЕАЭС 2025) [Электронный ресурс] // Евразийская экономическая комиссия. URL: https://eec.eaeunion.org/digital/ (дата обращения: 28.11.2025).

2. CREST International Accreditation Framework. Standards and Governance Structure [Electronic resource] // CREST International. URL: https://www.crest-approved.org/standards/ (дата обращения: 28.11.2025).

3. EU Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council) [Electronic resource] // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата обращения: 28.11.2025).

4. ISO/IEC 27001:2022 Information Security Management Systems. Requirements [Electronic resource] // International Organization for Standardization. URL: https://www.iso.org/standard/82875.html (дата обращения: 28.11.2025).

5. Next Generation Firewall Market and Technology Review 2024 [Electronic resource] // Gartner Research. URL: https://www.gartner.com/en/documents/ngfw-2024 (дата обращения: 28.11.2025).

6. The NIST Cybersecurity Framework (CSF) 2.0. Final Version 2024 [Electronic resource] // National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата обращения: 28.11.2025).

7. Global Cybersecurity Capacity Building Report 2024 [Electronic resource] // United Nations Open-Ended Working Group on ICT Security. URL: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2024/09/oewg-capacity-report.pdf (дата обращения: 28.11.2025).

8. ENISA Cybersecurity Certification Reports 2023–2024 [Electronic resource] // European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/topics/certification (дата обращения: 28.11.2025).

Пичугин Николай Васильевич
Младший научный сотрудник
Центр политических исследований и прогнозов,
Институт Китая и современной Азии РАН
E-mail: nikolaivpichugin@yandex.ru

Pichugin Nikolai Vasilievich,
Junior Researcher,
Center for Political Research and Forecasts,
Institute of China and Contemporary Asia of the Russian Academy of Sciences
E-mail: nikolaivpichugin@yandex.ru

СЕРВИСНАЯ СИСТЕМА ЖАЛОБ НАСЕЛЕНИЯ – ОСНОВА ДЛЯ САМОРЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КНР

THE SERVICE SYSTEM OF COMPLAINTS OF POPULATION – THE BASIS FOR SELF-REGULATION OF THE INFORMATION SPACE OF THE PRC

Аннотация. Автором раскрыта роль сервисной системы жалоб населения в процессе саморегулирования информационного пространства Китайской Народной Республики. Продемонстрированы особенности институционального функционирования и правового регулирования сервисной системы. Выделены направления развития сервисной системы на 2025 г.

Ключевые слова: КНР, сервисная система, саморегулирование, специальные кампании, нормативное правовое регулирование.

Abstract. The author reveals the role of the service system of complaints of the population in the process of self-regulation of the information space in the People's Republic of China. The institutional functioning and legal regulation of the service system are demonstrated. Directions for the service system's development through 2025 are outlined.

Key words: PRC, service system, self-regulation, special campaigns, legal regulation.

Сервисная система жалоб населения на нарушения в сети Интернет (сервисная система) функционирует на основе многоуровневой модели цифрового управления Китайской Народной Республики (КНР), в которой регулирующие функции распределены между партийными, государственными органами, а также квазигосударственными институтами. Данные структуры взаимодействуют посредством специализированных онлайн-платформ.

На партийном уровне сервисная система централизована под управлением Государственной канцелярии интернет-информации КНР, в ведении которой находится Центр по выявлению нездоровой и незаконной информации (ЦВННИ). Сотрудники Всекитайской канцелярии по борьбе с порнографией, нелегальной печатной, аудио- и видеопродукцией также несут ответственность за обеспечение работы ЦВННИ. Национальная интеллектуальная платформа для сбора сообщений об организованной преступности функционирует обособленно под управлением Национальной канцелярии КНР по борьбе с организованной преступностью.

Отдельно следует выделить Онлайн-платформу для приема жалоб и опровержения слухов, связанных с армией и Онлайн-платформу для сообщения о преступлениях и вредоносной информации, связанной с армией. Работа указанных платформ координируется представителями Государственной канцелярии интернет-информации КНР. Однако поскольку они регулируют категории нарушений в информационном пространстве, связанные непосредственно с НОАК, то имеют отличии в функционировании. Например, могут быть смягчены требования к подтверждению личности при подаче жалоб.

На государственном уровне Министерство общественной безопасности КНР и находящиеся в его подчинении сотрудники Сетевой полиции обеспечивают работу Платформы для сообщений о преступлениях в сети Интернет. В ведении Министерства промышленности и информатизации КНР действует узкопрофильный Центр приема жалоб пользователей телекоммуникаций. Министерство культуры и туризма КНР координирует работу Онлайн-системы сбора и обработки жалоб на национальном рынке культуры и туризма, что подчеркивает высокие темпы цифровизации китайского рынка культуры на современном этапе. Министерство образования КНР совместно с Государственным комитетом по делам здравоохранения КНР принимают активное участие в обеспечении функционирования Совместной платформы по опровержению слухов в Китае. Борьба против фабрикации и распространения слухов связана с использованием слухов в качестве внутриполитического инструмента, характерным для КНР.

На квазигосударственном уровне следует выделить Центр приема сообщений о вредоносной информации и спаме в сети Интернете (ЦСВИС). Деятельность указанного ведомства координируется Министерством промышленности и информатизации КНР, но также обеспечивается представителями Интернет-сообщества Китая. По инициативе данной квазигосударственной организации ЦСВИС был создан в 2008 г. [1].

Диверсификация регулирующих функций между представленными ведомствами и подчиняющимися им онлайн-платформами соответствует широкому спектру категорий

нарушений в сети Интернет, по которым можно подать жалобы в рамках сервисной системы. Одновременно повышается скорость и качество обработки отчетов о противоправной деятельности. В результате, выбор корректной категории нарушения отчитывающимся субъектом в китайской сервисной системе является одним из ключевых условий принятия жалобы.

Специальные кампании по регулированию информационного пространства КНР, также являющиеся механизмом саморегулирования, проводятся при использовании сервисной системы. В период реализации специальных кампаний, китайские граждане стимулируются к участию в системе общественного саморегулирования через правовые механизмы материального поощрения за достоверные сообщения о противоправной деятельности в информационном пространстве. В процессе реализации специальных кампаний ответственные органы в открытом доступе публикуют так называемые «типичные примеры» (典型案例) выявленных и пресеченных нарушений. Ориентируясь на них, заинтересованные лица могут более эффективно вести мониторинг, легализовывать и направлять отчеты о нарушениях в китайском сегменте сети Интернет.

Следуя принципу гласности, информация о запуске специальных кампаний, таких как, например, «Чистая и прозрачная сеть» (清朗行动) своевременно публикуется в официальных СМИ. В случае необходимости, с помощью обнародования «типичных примеров» китайские регуляторы могут направлять пользователей сервисной системы на поиск определенных категорий нарушений. Функционирование сервисной системы позволяет отслеживать как степень исполнения действующих плановых, нормативных правовых и подзаконных актов, так и корректировать, с учетом установленных новых форм противозаконной деятельности, готовящиеся правовые документы.

Особенности нормативного правового регулирования – являются одним из ключевых элементов, способствующих устойчивому функционированию сервисной системы. Подзаконные акты регламентируют строгий порядок материального стимулирования отчитывающихся субъектов [2]. Он включает фиксированные высокие минимальные и максимальные ставки вознаграждений в зависимости от категории нарушений, а также четкий порядок и процедуру их выплаты. Дополнительно устанавливаются специальные формулы для расчета вознаграждений для отчетов о наиболее серьезные категории противозаконной деятельности. Как правило, итоговая сумма выплат рассчитывается в процентном соотношении с учетом стоимости конфискованного у преступников имущества или оборота преступной деятельности.

Отдельно на правовом уровне установлены механизмы правовой защиты информаторов. В регулирующих актах закреплена юридической ответственность за преднамеренное распространение заведомо-недостоверных сведений о предполагаемых нарушениях в сети Интернет [3; 4]. Указанное, в сочетании с требованиями по подтверждению личности с использованием удостоверения гражданина КНР и указанию доказательств при подаче отчета, минимизирует риск фабрикации передаваемой информации.

Развитие сервисной системы на современном этапе ведется по двум основным направлениям. Во-первых, в 2026 г. планируется проведение реформы так называемых «комплексных центров управления» (综治中心) [5]. Предполагается, что их работа будет обеспечивать функционирование сервисной системы на четырех уровнях: уездном, поселковом, муниципальном и региональном. Сотрудники данных центров не ограничиваются аккумулированием и обработкой жалоб о нарушениях, исключительно связанных с регулированием информационного пространства КНР. В совокупности функционирование центров направлено на поддержание общественной безопасности и превентивное управление социальными рисками.

Во-вторых, в КНР происходит стремительное развитие таких сфер, как создание и регулирование национального рынка данных. В соответствующих нормативных правовых актах по отношению операторам данных устанавливаются требования по созданию каналов подачи жалоб в отношении их деятельности [6; 7]. Регламентируются принципы работы данных институтов. В перспективе возможно создание отдельной онлайн-платформы, специализирующейся на обработке отчетов о таких противоправных актах, как невыполнение требований к безопасности данных, кража данных, незаконный сбор и распространения данных, нарушение прав интеллектуальной собственности.

Заключение. Сервисная система жалоб населения на нарушения в сети Интернет наряду и в сочетании со специальными кампаниями является действующим управленческим инструментом по регулированию информационного пространства КНР. На современном этапе китайские власти проводят меры по централизации сервисной системы и ее расширению с учетом реализуемых направлений цифрового строительства (национальный рынок данных). Распределение регулирующих функций между узкопрофильными онлайн-платформами и координирующими их деятельность партийными, государственными и квазигосударственными ведомствами позволяет регулировать широкий перечень нарушений. Руководствуясь принципом гласности, китайские власти могут фокусировать внимание граждан на поиске и отправке отчетов об определенных формах противоправной деятельности. На правовом уровне за счет строго

регламентированных механизмов выплат за достоверные жалобы, защиту отчитывающихся субъектов обеспечивается стимулирование граждан к саморегулированию китайского сегмента сети Интернет.

Список источников и литературы:

1. 网络不良与垃圾信息举报受理中心[Центр приёма и передачи сообщений о сетевой небезопасности и спаме]. URL: https://www.12321.cn/single?tpl=institution (дата обращения: 07.10.2025).
2. “扫黄打非”工作举报奖励办法 [Меры поощрения за сообщения по теме «борьба с порнографией и незаконными публикациями]. 中国扫黄打非网[*Китайская сеть по борьбе с порнографией и незаконными публикациями*], 20.01.2025. URL: https://www.shdf.gov.cn/shdf/contents/708/388912.html (дата обращения: 07.10.2025).
3. 中华人民共和国刑法 [Уголовный кодекс КНР]. URL: https://www.pkulaw.com/chl/3b70bb09d2971662bdfb.html (дата обращения: 07.10.2025).
4. 中华人民共和国治安管理处罚法 [Закон КНР о наказаниях в сфере общественной безопасности]. URL: https://clck.ru/3MnY9V (дата обращения: 07.10.2025).
5. 中央政法委：2026 年基本实现省、市、综治中心视范化 [Центральная политико-юридическая комиссия: к 2026 г. стандартизация провинциальных, муниципальных и поселковых комплексных центров управления будет в основном достигнута]. 新华社 [*Агентство Синьхуа*], 31.03.2025. URL: https://gszfw.gov.cn/Wap/Show/435037 (дата обращения: 07.10.2025).
6. 网络数据安全管理条例 [Правила управления безопасностью сетевых данных] // 国务院 [Госсовет КНР], 24.09.2024. URL: https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm (дата обращения: 07.10.2025).
7. 政务数据共享条例 [Правила совместного использования правительственных данных] // 国务院公报 [Информационное агентство Госсовета], 03.06.2025. URL: https://www.gov.cn/gongbao/2025/issue_12106/202506/content_7028417.html (дата обращения: 07.10.2025).

Иван Владимирович Попович,
студент 1 курса магистратуры направления
«Международное регионоведение»,
Дипломатическая академия МИД России,
E-mail: popovich.i2019@gmail.com

Ivan V. Popovich,
first year student at the master’s program,
Diplomatic Academy of the Russian Ministry of Foreign Affairs,
E-mail: popovich.i2019@gmail.com

КРИЗИС МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАЛТИЙСКОМ РЕГИОНЕ

INTERNATIONAL INFORMATION SECURITY CRISIS IN THE BALTIC REGION

Аннотация: Автором раскрыты основные предпосылки и проявления международного информационного противостояния в Балтийском регионе. Оцениваются перспективы дальнейшего развития ситуации и рассматриваются возможные пути укрепления информационной безопасности России.

Ключевые слова: Балтийский регион, Прибалтика, информационная безопасность, кибератаки, КИИ, НАТО, СВО.

Abstract: The author covers the main prerequisites and manifestations of the international information confrontation in the Baltic region. Various prospects for the further development of the situation are assessed, and possible ways of strengthening the information security of Russia are considered.

Key words: Baltic region, Baltic States, information security, cyber attacks, critical information infrastructure, NATO, special military operation.

Кризис международного сотрудничества в Балтийском регионе как основа кризиса информационной безопасности. Значительная международная напряжённость в Балтийском регионе имеет место еще со времён распада Советского Союза. Так, сразу после получения независимости государства Прибалтики – Латвия, Литва и Эстония – отказались от участия в основных интеграционных процессах постсоветского пространства и приступили к укреплению своих международных позиций, зачастую опираясь на принципы национализма и критического отношения к России [2]. Напряженность в регионе продолжала расти с поочередным вступлением расположенных на его территории

государств в НАТО, к чему руководство Российской Федерации обоснованно относилось с подозрением и открытой критикой.

С 2014 года отношения между Россией и другими государствами Балтийского региона перешли в стадию открытого антагонизма. Против Москвы были введены санкции под эгидой ЕС, в связи с чем объемы международной торговли в регионе существенно сократились. Осуждение странами Запада действий России в отношении Украины было использовано в качестве оправдания для активизации хакерских атак на критическую информационную инфраструктуру России в различных регионах страны, включая Калининград и Калининградскую область. В свою очередь, антагонистично настроенные к Москве государства Балтийского региона начали сообщать об ответных атаках, наносимых «пророссийскими» хакерскими группировками.

С начала российской СВО на территории Украины в 2022 году отношения России и остальных государств Балтийского региона находятся в самой высокой за постсоветский период точке напряженности. Ситуация осложняется тем, что со вступлением Финляндии и Швеции в Североатлантический альянс число угроз российским интересам в регионе существенно возросло. Присутствие России на Балтике стремятся сократить, ведя против нашей страны информационную войну, описывая Балтийское море как сферу интересов или даже «внутреннее море» НАТО.

Средства и угрозы информационного противостояния в Балтийском регионе. Одним из наиболее распространенных методов информационного противостояния на Балтике, как и в других регионах, являются хакерские атаки на критическую инфраструктуру, направленные на слив или уничтожение ценной информации, либо на достижение иных результатов. Из российских объектов таким атакам в Балтийском регионе преимущественно подвергаются официальные сайты органов власти и частных предприятий Калининградской области, находящейся в особенно уязвимом состоянии из-за географической изолированности от остальной части России [1]. В Прибалтике и других Западных государствах региона состоящие из анонимных лиц хакерские группировки также атакуют критическую информационную инфраструктуру, нанося ущерб репутации государственных органов и отдельных официальных лиц [6]. В перспективе подобные атаки с обеих сторон могут проводиться для оценки слабых и сильных сторон КИИ противника перед возможным полномасштабным конфликтом [5].

Отдельным полем информационной борьбы, выходящим далеко за рамки виртуального конфликта, является ситуация с повреждением трубопроводов и кабелей на дне Балтийского моря, используемая как одно из оправданий для противостояния так называемому «теневому флоту» России. Причастность Москвы к нанесению ущерба

подводной инфраструктуре стран Запада в регионе так и не была доказана. Несмотря на это, различные СМИ, действующие в интересах антироссийски настроенных акторов, продвигают перед широкой публикой ничем не подтвержденный нарратив о том, что именно Россия целенаправленно повреждает кабели и трубопроводы на дне Балтийского моря. Наиболее одиозным примером этой кампании можно назвать выдвижение Москве неофициальных обвинений в подрыве собственных газопроводов «Северный поток-1» и «Северный поток-2» [4].

Данная антироссийская информационная кампания также имеет важное и неприемлемое для России практическое значение – дискредитация российского судоходства в регионе с целью ограничения международной торговли нашей страны и дальнейшей изоляции Калининградской области.

Возможные пути развития информационного противостояния в Балтийском регионе. Оценивая перспективы развития международного информационного конфликта на Балтике, необходимо учитывать региональный контекст в более широком понимании [3]. Так, до завершения российской СВО на территории Донбасса, убедительных предпосылок чему на данный момент не наблюдается, существенное улучшение отношений между Москвой и Западом практически невозможно. Следовательно, в краткосрочной и среднесрочной перспективе кризис международной информационной безопасности в Балтийском регионе сохранится. Его прежние проявления сохранятся, могут появиться и новые. И даже завершение СВО не приведет к быстрому снижению напряженности.

Следовательно, для защиты критической информационной инфраструктуры России необходимо продолжать развитие средств защиты от кибератак, а также обращаться к иным необходимым средствам. Также следует продолжить конструктивную работу по формированию позитивного образа России за рубежом, в том числе и в Балтийском регионе, с использованием как привычных СМИ («RT», «Sputnik»), так и иных механизмов.

Заключение. Итак, кризис информационной безопасности в Балтийском регионе следует воспринимать как составляющую общего международного кризиса, основанного на противостоянии между Россией и блоком НАТО, недружественно настроенным к ней. В рамках информационного конфликта стороны стремятся укрепить собственную безопасность и проверить готовность противника к потенциальной войне. Со стороны Запада противостояние несет также элементы экономической конкуренции, в которой используются незаконные и неэтичные методы борьбы.

Сохранение международной напряженности и перспектива ее дальнейшей эскалации требует от нашей страны укрепления безопасности объектов КИИ, грамотного ведения противостояния информационным угрозам. Также важно понимать, что в текущих

условиях укрепление информационной безопасности находится в прямой связи с усилением безопасности военного характера, поскольку войны XXI века ведутся не только на полях сражений, но и мировом информационном пространстве.

Список источников и литературы:

1. Власти: в Калининграде идет хакерская атака на операторов сотовой связи [Электронный ресурс] // РБК URL: https://kaliningrad.rbc.ru/kaliningrad/24/10/2025/68fb47329a7947ab48dc9590?ysclid=mhw29lm4hc268068103 (дата обращения: 11.11.2025)
2. Информационный фронт Эстонии [Электронный ресурс] // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnyy-front-estonii/ (дата обращения: 11.11.2025)
3. Кириленко В. П., Алексеев Г. В. Политические технологии и международный конфликт в информационном пространстве Балтийского региона // Балтийский регион. 2018. Т. 10, № 4. С. 20-38.
4. Кремль назвал абсурдным обвинение России в ЧП на «Северных потоках» [Электронный ресурс] // РБК URL: https://www.rbc.ru/politics/18/10/2022/634e6e1e9a794714d2f6e633?ysclid=mhw2c8vx5u564304524 (дата обращения: 11.11.2025)
5. Трансформация Балтийского региона: от пространства сотрудничества к зоне риска [Электронный ресурс] // РСМД. URL: https://russiancouncil.ru/analytics-and-comments/analytics/transformatsiya-baltiyskogo-regiona-ot-prostranstva-sotrudnichestva-k-zone-riska/ (дата обращения: 11.11.2025)
6. Хакеры «отомстили» за Крым: армия Литвы готовится к «аннексии Калининграда» [Электронный ресурс] // МК URL: https://www.mk.ru/politics/2015/06/11/khakery-nato-gotovitsya-k-anneksii-kaliningrada.html?ysclid=mhvtwaxy1r192987529 (дата обращения: 11.11.2025)

Екатерина Дмитриевна Ракова,
студент бакалавриата департамента международных отношений Международной академии бизнеса и управления
E-mail: volama@bk.ru

Ekaterina D. Rakova,
Bachelor's student in the Department of International Relations at the International Academy of Business and Management
Email: volama@bk.ru

СТРАТЕГИЧЕСКОЕ ПАРТНЕРСТВО РОССИИ И ИРАНА В ИКТ-СРЕДЕ: ПРОТИВОДЕЙСТВИЕ ГЛОБАЛЬНЫМ УГРОЗАМ И ПЕРСПЕКТИВЫ ВСЕОБЪЕМЛЮЩЕГО СОТРУДНИЧЕСТВА

RUSSIA-IRAN STRATEGIC PARTNERSHIP IN ICT ENVIRONMENT: COUNTERING GLOBAL THREATS AND PROSPECTS FOR COMPREHENSIVE COOPERATION

Аннотация. Доклад посвящен анализу стратегического партнерства между Российской Федерацией и Исламской Республикой Иран в сфере информационной безопасности. Рассматривается подписанное в 2021 году межправительственное соглашение как ключевой инструмент противодействия общим угрозам, исходящим от «коллективного Запада», включая кибератаки, дезинформационные кампании и вмешательство во внутренние дела. Особое внимание уделяется механизмам реализации соглашения: созданию совместных центров реагирования на киберинциденты (SOC), обмену технологиями и координации в международных организациях.

В работе также раскрывается роль цифровой публичной дипломатии и культурного сотрудничества как элементов «мягкой силы», способствующих укреплению взаимного доверия между странами. Подчеркивается взаимосвязь между сотрудничеством в сфере ИКТ и подготовкой к подписанию Всеобъемлющего договора о стратегическом партнерстве. Доклад завершается оценкой перспектив российско-иранского взаимодействия в контексте формирования многополярной модели международных отношений и снижения уязвимости критической информационной инфраструктуры обеих стран.

Ключевые слова: Стратегическое партнерство, информационная безопасность, ИКТ, ИКТ-среда, Российско-иранские отношения, международная информационная безопасность, цифровой суверенитет, киберугрозы, соглашение о сотрудничестве, всеобъемлющее сотрудничество.

Abstract. This report analyzes the strategic partnership between the Russian Federation and the Islamic Republic of Iran in the field of information security and ICT. The intergovernmental agreement signed in 2021 is considered a key tool for countering common threats emanating from the "collective West," including cyberattacks, disinformation campaigns, and interference in internal affairs. Particular attention is paid to the mechanisms for implementing the agreement: the creation of joint cyber incident response centers (SOCs), technology exchange, and coordination within international organizations.

The paper also explores the role of digital public diplomacy and cultural cooperation as elements of "soft power" that contribute to strengthening mutual trust between the countries. The relationship between cooperation in cybersecurity and preparations for the signing of the Comprehensive Strategic Partnership Agreement is emphasized. The report concludes with an assessment of the prospects for Russian-Iranian cooperation in the context of the formation of a multipolar model of international relations and reducing the vulnerability of the critical information infrastructure of both countries.

Key words: Strategic partnership, information security, ICT, ICT environment, Russian-Iranian relations, international information security, digital sovereignty, cyber threats, cooperation agreement, comprehensive cooperation.

Введение. В условиях стремительной цифровизации и роста киберугроз – от фейков до хакерских атак – международное сотрудничество становится ключевым инструментом защиты суверенитета. В 2021 году Россия и Иран подписали соглашение о сотрудничестве в области информационной безопасности [7], ставшее ответом на агрессивные действия в цифровом пространстве. Этот документ не только закрепляет совместное противодействие «коллективному Западу», но и формирует основу для стратегического партнёрства, включая подготовку Всеобъемлющего договора. Цель работы - определить роль этого документа в развитии стратегического альянса, что требует анализа его структуры, угроз, на которые он направлен, и его влияния на подготовку и подписание Всеобъемлющего договора о сотрудничестве.

ИКТ- среда как основа доверия. Соглашение 2021 года [7], подписанное Сергеем Лавровым и Мохаммадом Джавадом Зарифом, стало ответом на системные угрозыакие как хакерские атаки и дезинформационные кампании Запада. Как отмечалось в предыдущей работе автора, документ предусматривает:

–Координацию действий [6] в борьбе с киберпреступностью, включая совместные расследования и обмен данными о компьютерных инцидентах.

–Технологическую поддержку: Россия экспортирует в Иран IT-решения, включая системы анализа аудиоданных на базе ИИ и платформы для цифровизации бизнес-процессов.

–Создание SOC-центров (Security Operations Center), которые повышают защищённость критической инфраструктуры, например, транспортного коридора «Север-Юг».

Этот документ стал логичным продолжением Договора 2001 года [1], заложившего основы сотрудничества, но адаптированным к вызовам цифровой эпохи.

Культурная дипломатия: цифровые мосты между народами. Культурное взаимодействие, как часть «мягкой силы», играет ключевую роль в укреплении доверия. В статье [5] подробно описываются проекты, реализуемые обеими странами:

–Онлайн-образование:

Платформа Persian Language Online, поддерживаемая Фондом наследия Ирана, предлагает бесплатные курсы персидского языка, что способствует популяризации иранской культуры среди россиян.

Российский проект LectOrient предоставляет лекции по истории, философии и литературе Ирана, создавая основу для межкультурного диалога.

–Оцифровка культурного наследия:

Российские и иранские музеи совместно оцифровывают коллекции, например, проводят виртуальные туры по экспозициям, что расширяет аудиторию и противодействует стереотипам.

Издательства («Садра», «Медина») публикуют в открытом доступе произведения персидской литературы, такие как «Шахнаме» Фирдоуси, с параллельным переводом на русский язык.

Эти инициативы, как отмечает Ракова Е.Д. [5], «стирают барьеры между народами», подчеркивая общность истории и менталитета. Например, сходство славянских и персидских языковых корней (индоевропейская семья) становится основой для лингвистических проектов.

Информационное противодействие и «цифровой суверенитет». Оба государства активно борются с западной дезинформацией, используя схожие методы:

–Создание альтернативных информационных платформ:

Иран блокирует доступ к западным соцсетям, продвигая национальные аналоги (например, «Soroush»), а Россия развивает экосистему VK и «Рутуб».

Совместные медиапроекты, такие как телеканал IRIB Russia, транслируют новости на русском и персидском языках, формируя объективную картину событий.

–Продвижение «правдивой информации»:

Как мы знаем, «цифровая дипломатия эффективна лишь при нейтрализации радикальных групп». Например, Фонд Ибн Сины проводит вебинары, разоблачающие мифы об исламе и иранской политике. Эти меры не только защищают суверенитет, но и создают основу для альтернативной глобальной повестки, противопоставленной западной гегемонии.

Заключение. Результаты сотрудничества уже очевидны: укрепление правовой базы, снижение уязвимости инфраструктур и рост взаимного доверия. Культурные инициативы, такие как онлайн-мероприятия, стали мостом между обществами, а координация в ШОС и ООН усилила влияние обеих стран на формирование глобальных норм кибербезопасности. Перспективы связаны с подготовкой Всеобъемлющего договора, который расширит сотрудничество до обороны, экономики и технологий. Это не только укрепит позиции России и Ирана как центров многополярного мира, но и продемонстрирует, что совместное противостояние цифровым вызовам способно стать основой стратегического союза. Таким образом, соглашение 2021 года не просто ответ на угрозы, а шаг к новому уровню партнёрства, где кибербезопасность становится фундаментом для устойчивого диалога в условиях глобальной нестабильности. Исследование базируется на анализе текста соглашения, сравнении с аналогичными договорами, например, с Китаем [2] и оценке медийных и научных источников. Ключевые угрозы, выделенные в документе, включают вмешательство во внутренние дела, терроризм и разрушение критической инфраструктуры. В ответ на них стороны договорились об обмене данными, совместных расследованиях, поддержке ИТ-разработок и координации в международных организациях, таких как ООН и ШОС. Особое внимание уделяется практическим шагам: созданию центров реагирования на киберугрозы (SOC), экспорту российских технологий и интеграции культурной дипломатии как элемента «мягкой силы». Ратификация соглашения при новом президенте Ирана подчеркнула преемственность и приоритет отношений с Россией, а ранее достигнутые договорённости в сфере ИТ и телекоммуникаций заложили основу для технологического партнёрства. Результаты исследования подтверждают, что соглашение 2021 г. укрепило правовую базу для противодействия киберугрозам и усилило доверие между странами. Культурная дипломатия, включая онлайн-лекции и совместные проекты, сыграла ключевую роль в сближении народов, а координация в международных организациях повысила влияние обеих стран на формирование глобальных норм кибербезопасности. Практическая значимость работы заключается в определении

снижения уязвимости инфраструктур и подготовки почвы для Всеобъемлющего договора, который охватывает оборону, безопасность и экономику. Перспективы сотрудничества связаны с развитием ИТ и защитой критических объектов, что укрепит позиции России и Ирана как центров многополярного мира. Таким образом, соглашение стало катализатором стратегического партнёрства, доказав, что совместное противостояние цифровым вызовам способно стать основой долгосрочного союза в условиях глобальной нестабильности.

Список источников и литературы:

1. Договор об основах взаимоотношений и принципах сотрудничества между Российской Федерацией и Исламской Республикой Иран от 12 марта 2001 г. http://kremlin.ru/supplement/3290 (Дата обращения: 01.11.2025).

2. Договор о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой от 25 января 2002 года https://docs.cntd.ru/document/901792686?marker (дата обращения 01.11.2025).

3. Доктрина по информационной безопасности Российской Федерации от 6 декабря 2016 года http://kremlin.ru/acts/bank/41460 (дата обращения 01.11.2025).

4. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации утверждены Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г. http://www.scrf.gov.ru/security/information/document155/ (дата обращения 01.11.2025).

5. Ракова Е.Д. Цифровая публичная дипломатия между Россией и Ираном, Digitalorientalia 2023, Vol. 3, No. 3-4.

6. Сетевое издание «Коммерсантъ» Тегеранская преференция. Технологический сектор России предложил Ирану партнерство, Т.Исакова, Н.Королев, Ю.Тишина, Н.Скорлыгина, https://www.kommersant.ru/doc/6084928?ysclid=ltprrotwrn817378390 (дата обращения: 01.11.2025).

7. Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности от 26 января 2021 года https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/59914/ (Дата обращения: 01.11.2025).

8. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности https://docs.cntd.ru/document/420283259 (дата обращения 01.11.2025).

Анастасия Игоревна Суховерхова,
магистрант 1 курса факультета Международные отношения,
Дипломатическая академия МИД России,
E-mail: anastasia.s10@yandex.ru

Anastasia I. Sukhoverkhova,
first-year master's student in the Faculty of International Relations,
Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation,
Email: anastasia.s10@yandex.ru

ОСОБЕННОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГЕРМАНИИ

FEATURES OF THE INFORMATION SECURITY SYSTEM IN GERMANY

Аннотация. В статье проанализированы основные нормативно-правовые акты, формирующие правовую основу кибербезопасности Германии, рассмотрены ключевые принципы германской Стратегии кибербезопасности. Особое внимание уделено роли Федерального управления по информационной безопасности как центрального органа координации. Сделан вывод, что германская модель кибербезопасности отличается системностью, институциональной согласованностью и ориентацией на международные стандарты, обеспечивая высокий уровень киберустойчивости и доверия к цифровой среде. Опыт Германии может служить ориентиром для построения эффективных национальных стратегий кибербезопасности в других европейских странах.

Ключевые слова: кибербезопасность, Германия, Федеральное управление по информационной безопасности, нормативно-правовое регулирование, цифровой суверенитет, персональные данные, критическая инфраструктура, кибератаки.

Abstract: The article analyzes the key legal framework for cybersecurity in Germany and examines the key principles of the German Cybersecurity Strategy. Particular attention is paid to the role of the Federal Office for Information Security as the central coordinating body. It concludes that the German cybersecurity model is characterized by its systemic nature, institutional coherence, and alignment with international standards, ensuring a high level of cyber resilience and trust in the digital environment. Germany's experience can serve as a benchmark for developing effective national cybersecurity strategies in other European countries.

Key words: cybersecurity, Germany, Federal Office for Information Security, legal framework, digital sovereignty, personal data, critical infrastructure, cyberattacks.

Современное развитие цифровых технологий сопровождается не только ростом инновационного потенциала, но и увеличением масштабов и сложности киберугроз, способных нанести значительный ущерб государственным структурам, экономике и гражданскому обществу. В этих условиях обеспечение кибербезопасности становится одной из ключевых составляющих национальной безопасности. Германия, являясь технологическим и экономическим лидером Европейского союза, выстраивает комплексную систему правового и институционального регулирования в сфере информационной безопасности.

Цель настоящего исследования заключается в рассмотрении нормативно-правовой базы кибербезопасности Германии, а также в анализе основных стратегических направлений и принципов, определяющих политику государства в данной области. Рассмотрение подобных документов позволяет выявить особенности германского подхода к обеспечению киберустойчивости, его соответствие общеевропейским стандартам, а также тенденции развития национальной модели кибербезопасности в контексте глобальных цифровых трансформаций.

Нормативно-правовая база ФРГ в области информационной безопасности. Основу кибербезопасности Германии составляют несколько ключевых нормативно-законодательных актов. Среди них можно выделить Стратегию кибербезопасности, Федеральный закон о защите данных**,** Общий регламент о защите данных**,** Закон о повышении безопасности информационных технологий в двух версиях от 2015 г. и 2021 г.

Последняя версия Стратегии кибербезопасности была опубликована в 2021 г. Важен тот факт, что данный документ является частью стратегии информационной безопасности Евросоюза. В Стратегии определены основополагающие долгосрочные направления политики правительства Германии в области кибербезопасности в форме руководящих принципов, направлений деятельности и стратегических целей.

Стратегия кибербезопасности 2021 года определяет четыре основополагающих руководящих принципа:

1) формирование кибербезопасности как общей ответственности правительства, бизнеса, общества и академических кругов и общества;

2) укрепление цифрового суверенитета правительства, бизнеса, академических кругов и общества;

3) безопасное формирование цифровизации;

4) разработка измеримых и прозрачных целей [3].

Первое направление нацелено на повышение осведомленности общественности, повышение «информационной грамотности» граждан и укрепление защиты прав потребителей в цифровом мире [3, с. 22].

Второй принцип направлен на укрепление кибербезопасности экономики в целом, а также на критически важную инфраструктуру. Особое внимание уделяется малым и средним предприятиям, а также расширении сотрудничества между правительством и промышленностью и развитию нормативно-правовой базы для бизнеса. Цели, способствующие развитию ключевых и будущих технологий, направлены на укрепление цифрового суверенитета и конкурентоспособности компаний в сфере кибербезопасности [3, с. 22-24].

Третий принцип способствует снижению барьеров для эффективного сотрудничества между органами власти, выявлению постоянно меняющихся требований в киберпространстве и соответствию данным требованиям [3, с. 25].

Четвертый принцип посвящен участию Германии в европейской и международной политике информационной безопасности. ФРГ стремиться развивать основы и инструменты политики кибербезопасности ЕС и НАТО. Кроме того, федеральное правительство выступает за укрепление международной нормативно-правовой базы для государств в киберпространстве и международной борьбы с киберпреступностью [3, с. 25-26]. Так как Германия входит в ЕС, на ее территории также действует Общий регламент о защите данных, который нацелен на защиту персональных данных, в дополнение, согласно Регламенту, накладываются штрафы за утечки данных [6]. Наряду с общеевропейским законом в ФРГ существует собственный Федеральный закон о защите данных, который регулирует обработку персональных данных государственными органами и частными организациями, устанавливая правила сбора, хранения и использования данных [1]. ФРГ стремится развивать защиту критически важной инфраструктуры с помощью современных технологий. Для выполнения этой цели планируется уделять больше внимания безопасности цепочек поставок ИТ-решений в правовых нормах, регулирующих критически важную инфраструктуру, а также предлагать проекты по повышению осведомлённости и киберустойчивости. В этой связи целесообразно более детально рассмотреть вышеупомянутые законы о повышении безопасности информационных технологий. Закон о повышении безопасности информационных технологиях от 2015 г. обязал операторов критической инфраструктуры (энергетика, водоснабжение, финансы, транспорт и др). соответствовать минимальным стандартам безопасности, внедрять системы защиты и сообщать о киберинцидентах в Федеральное управление по

информационной безопасности (BSI) [5]. Вторая редакция закона от 2021 г. значительно расширяет полномочия BSI, в особенности, по выявлению уязвимостей безопасности и защите от кибератак. Закон содержит положение, запрещающее использование критически важных компонентов для защиты общественного порядка или безопасности в Германии. Операторы сетей также должны соответствовать заранее определенным высоким требованиям безопасности, а критически важные компоненты должны быть сертифицированы. Компании, представляющие особый общественный интерес (например, производители оружия или компании, имеющие важное экономическое значение), также будут обязаны внедрять определенные меры ИТ-безопасности и будут включены в конфиденциальный обмен информацией с BSI [7].

Федеральное управление по информационной безопасности. Для скоординированной реакции на киберугрозы BSI играет роль центрального контактного пункта для федерального и земельного правительств. Дальнейшее преобразование ведомства должно поспособствовать выстраиванию постоянного сотрудничества между всеми заинтересованными сторонами, а также созданию общей информационной системы.

В дополнительные полномочия ведомства входит ряд следующих функций:

1) исследование рисков безопасности при применении информационных технологий и разработку мер безопасности;

2) разработка критериев, процедур и инструментов для тестирования и оценки безопасности систем и компонентов информационных технологий;

3) поддержка федеральных агентств, ответственных за безопасность информационных технологий;

4) поддержка полиции и правоохранительных органов при выполнении ими своих уставных обязанностей, а также национальных разведывательных служб при оценке и анализе информации;

5) проведение аудитов безопасности телекоммуникационных систем, включая цифровые телекоммуникационные системы, в федеральных агентствах и компаниях, работающих по контрактам, связанным с федеральной секретной информацией [2].

Говоря о других институтах и органах в области кибербезопасности, можно выделить новую коммуникационную платформу, создаваемую на базе BSI. Платформа должна облегчить обмен информацией о кибератаках. Это станет ценным ресурсом, особенно для малых и средних предприятий, для устойчивого снижения ущерба от кибератак, таких как атаки программ-вымогателей. Кроме того, федеральное правительство намерено публично поощрять инвестиции частного сектора в повышение киберустойчивости малых и средних предприятий в секторах критической

инфраструктуры, а также уделять больше внимания безопасности цепочек поставок ИТ в законодательном регулировании критической инфраструктуры. Помимо упомянутой платформы в структуру BSI входит Национальный Центр кибербезопасности Германии, действующий как межведомственный хаб. В его работе участвуют представители Федеральной разведывательной службы, Федерального ведомства по защите конституции, Федеральной полиции и Министерства обороны. Целью работы является координация и быстрый обмен информацией о кибератаках [4].

Заключение. На сегодняшний день Германия сформировала достаточно разветвленную и устойчивую систему кибербезопасности, основанную на сочетании национального законодательства и общеевропейских правовых норм. Основные нормативные акты, регулирующие данную сферу, обеспечивают комплексный подход к защите информационной инфраструктуры, обработке персональных данных и противодействию киберпреступности. Можно предположить, что немецкая политика в области информационной безопасности в долгосрочной перспективе поспособствует укреплению цифрового суверенитета страны, развитию инновационных технологий и повышению уровня доверия общества к цифровой среде. Таким образом, германская модель кибербезопасности может рассматриваться как одна из наиболее сбалансированных и эффективных в Европе, обеспечивающая интеграцию национальных интересов с принципами коллективной безопасности Европейского союза.

Список источников и литературы:

1. Bundesdatenschutzgesetz [Electronic resourse] // Bundesamt für Justiz. 2017. URL: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html (дата обращения: 12.11.2025).
2. Cybersicherheitspolitik des Bundes [Electronic resourse] // Bundesministerium des Innern. 2025. URL: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html (дата обращения: 11.11.2025).
3. Cybersicherheitsstrategie für Deutschland [Electronic resourse] // Bundesministerium des Innern, für Bau und Heimat. 2021. URL: https://bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1 (дата обращения: 12.11.2025) , - 141 s.
4. Das Nationale Cyber-Abwehrzentrum [Electronic resourse] // Bundeskriminalamt. 2025. URL: https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html (дата обращения: 12.11.2025).

5. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme [Electronic resourse] // Bundesgesetzblatt. 2015. URL: https://www.bgbl.de/xaver/bgbl/start.xav#/switch/tocPane?_ts=1762955302391 (дата обращения: 12.11.2025).
6. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 [Electronic resourse] // Amtsblatt der Europäischen Union. 2016. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679 (дата обращения: 12.11.2025).
7. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme [Electronic resourse] // Bundesamt für Sicherheit in der Informationstechnik. 2021. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html (дата обращения: 12.11.2025).

Яникеева Инна Олеговна,
к.полит.н., научный сотрудник ЦКЕМИ,
НИУ ВШЭ,
E-mail: yanikeeva93@mail.ru

Inna O. Yanikeeva,
Ph.D, in Political Science, Centre for Comprehensive European and International Studies (CCEIS),
HSE University,
E-mail: yanikeeva93@mail.ru

КОНСТРУИРОВАНИЕ КИБЕРУГРОЗ В ДИСКУРСЕ США: КЕЙС АДМИНИСТРАЦИИ ДЖ. БАЙДЕНА

CONSTRUCTING CYBER THREATS IN THE US DISCOURSE: THE BIDEN ADMINISTRATION'S DISCOURSE' CASE

Аннотация. Автором раскрыты основные особенности дискурса администрации Дж. Байдена при конструировании киберугроз и его использовании в качестве инструмента внешнеполитического влияния США. Анализ основан на материалах американских государственных органов за период с января 2021 года по январь 2025 года, ранее собранных для научной статьи. Всего было отобрано 47 документов. Установлено, что образ киберугроз формируется в американском дискурсе не только как технологический риск, но и как социально-политическая конструкция, направленная на легитимацию международного давления и введения санкций. Для проведения анализа была использована теория секьюритизации, конструктивизм и критический дискурс-анализ, позволяющие выявить механизмы переведения задачи обеспечения кибербезопасности в одну из сфер геополитической борьбы.

Ключевые слова: кибербезопасность, киберугрозы, внешняя политика, США, критический дискурс-анализ, Китай, Россия, Иран, КНДР.

Abstract. The author reveals the key features of the Biden administration's discourse on constructing cyberthreats and its use as a tool of foreign policy influence. The analysis is based on materials of the US government agencies covering the period from January 2021 to January 2025, previously collected for a research article. A total of 47 documents were selected for analysis. It is established that the image of cyberthreats is formed in the American discourse not only as a technological risk but also as a sociopolitical construct aimed at legitimizing international pressure and the imposition of sanctions. The analysis draws on securitization theory, constructivism, and critical discourse analysis to identify the mechanisms by which cybersecurity issues become a sphere of geopolitical struggle.

Key words: cybersecurity, cyber threats, foreign policy, the US, critical discourse analysis, China, Russia, Iran, DPRK.

Конструирование угроз в цифровой среде. В условиях трансформации мировой политики и ускоренной цифровизации государства непрерывно разрабатывают, обновляют и дополняют свои национальные киберстратегии, при этом интерпретируя киберугрозы и киберриски в терминах национальной безопасности. Закономерно с каждым годом усиливается интерес к данной теме и со стороны научного сообщества [1, 2, 6].

Важно отметить, что за стремлением государств, особенно великих держав, обеспечить безопасность в цифровой среде могут скрываться гегемонистские устремления международных акторов, одним из которых являются США, что проявилось особенно ярко на примере их риторики в отношении Латинской Америки при администрации Дж. Байдена [3].

С конца 2010-х годов в американских стратегических документах закрепляется концепция «malign influence operations» по отношению к цифровой среде – внешнего злонамеренного вмешательства, охватывающая широкий спектр действий от кибершпионажа до манипуляций общественным мнением, в частности под надуманным предлогом российского вмешательства во внутренние дела США посредством информационных технологий [12]. Тем самым киберугрозы стали относиться не только к технической категории, но и трансформировались в элемент политической риторики, направленной на консолидацию союзников и оправдание оказываемого давления на соперников.

Дискурс США в отношении угроз в цифровой среде строится вокруг ключевого нарратива «защиты демократии». В американских официальных документах подчеркивается необходимость противодействия «авторитарным режимам», использующим технологии для «подрыва демократических институтов» [12, 13]. Соединенные Штаты позиционируют себя как гаранта «ответственного лидерства» в цифровой сфере, связывая вопросы технологий с ценностной повесткой и моральным превосходством. В результате формируется нормативная дихотомия: «демократический» и «авторитарный» подход в цифровой среде, где первый символизирует безопасность и открытость, моральное превосходство, а второй – угрозу и непрозрачность.

Особое место в американском дискурсе занимает тема искусственного интеллекта (ИИ) и его потенциального использования против демократических государств. Соединенные Штаты позиционируют развитие ИИ как фактор, требующий глобальной ответственности и прозрачности, противопоставляя себя странам, где ИИ рассматривается как элемент государственного контроля. Данный дискурс воспроизводится в официальных документах и выступлениях, где ИИ и кибербезопасность объединяются в единую линию в деле защиты демократических институтов [5].

Дискурс США тесно связан с логикой американского лидерства. Концепт «digital democracy» объединяет представления о свободе информации, рыночной экономике и высоких технологических стандартах [8]. Таким образом, экспорт демократических ценностей приобретает цифровое измерение – продвижение американских технологий становится элементом политического воздействия. Заявления о «защите демократии в Интернете» используются для оправдания мер контроля над цифровой инфраструктурой и давления на другие государства, что превращает информационную безопасность в инструмент геоэкономической и геополитической конкуренции. Так, заявляется о том, что американские технологии являются безопасными и продвинутыми, в отличие, например, от китайских, которые «не столь надежные» и «небезопасные», поскольку могут быть «использованы для шпионажа и других неприемлемых целей».

Другим важным аспектом является использование медиапространства и публичной дипломатии для закрепления создаваемого образа киберугроз. Посредством информационных кампаний США формируют глобальное восприятие киберугроз как вызова, исходящего от определенного круга государств (Россия, Китай, Иран и Северная Корея), тем самым создавая основания для консолидации союзников и введения мер против «нарушителей». В официальных заявлениях систематически воспроизводится нарратив о «злонамеренных акторах» в целях легитимации в глазах как внутренней, так и внешней аудитории политики США в сфере обеспечения безопасности в цифровой среде [9, 12, 13].

Секьюритизация киберугроз. В рамках дискурс-анализа американский нарратив о киберугрозах можно рассматривать как процесс секьюритизации. Он строится по классической схеме: агент (государство) обозначает некий объект как угрозу безопасности, приводит реципиенту (на кого направлен дискурс / кого стремятся убедить в «правильности» своего подхода) аргументы в пользу контрмер и получает право на исключительные меры [4, 7, 11, 13]. В данном случае речь идет о санкциях, ограничении технологического сотрудничества, контроле за экспортом и формировании коалиций

доверия в сфере цифровой политики, например Глобальное партнерство по искусственному интеллекту (Global Partnership on AI) [10]. Секьюритизация позволяет вывести вопрос из политической плоскости в сферу «экзистенциальной угрозы», что делает допустимыми меры, ранее считавшиеся спорными.

Так, дискурсивная стратегия США предполагает институционализацию угроз посредством правовых и дипломатических инструментов. Например, санкционные механизмы против России, Китая, Ирана и КНДР оформляются в логике борьбы с «киберпреступниками», «кибершпионажем» и «вмешательством в выборы» [5, 12]. Вашингтон использует тематику кибербезопасности как предлог для легитимации своей санкционной политики, дипломатического давления и технологического сдерживания конкурентов. Санкции, будучи представленными как ответные меры на нарушение международных норм, приобретают статус морально оправданного средства, направленного на «защиту открытого Интернета».

Заключение. Конструирование образа киберугроз в американском политическом дискурсе представляет собой многоуровневый процесс, сочетающий идеологические, нормативные и институциональные элементы. Киберугрозы секьюритизируются, а дискурс, сопровождающий обеспечение кибербезопасности, становится инструментом легитимации внешнеполитического давления на американских оппонентов. Соединенные Штаты используют это для укрепления своего лидерства и продвижения глобальной цифровой повестки, основанной на своих ценностях, в своих национальных интересах. При этом в долгосрочной перспективе американская стратегия способна привести к усилению фрагментации международной цифровой среды, росту недоверия к США и их технологиям, и усилению конфронтации между основными центрами силы на мировой арене.

Список источников и литературы:

1. Крутских А.В. Международная информационная безопасность: в поисках консолидированных подходов [Электронный ресурс] // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 342—351. URL: https://doi.org/10.22363/2313-0660-2022-22-2-342-351 (дата обращения: 11.11.2025).

2. Понька Т.И., Рамич М.С., У Ю. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация [Электронный ресурс] // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20, № 2. С. 382—394. URL: https://doi.org/10.22363/2313-0660-2020-20-2-382-394 (дата обращения: 11.11.2025).

3. Сокольщик Л.М., Яникеева И.О., Торопчин Г.В. ИКТ-безопасность во внешней политике США в отношении Латинской Америки: кейс дискурса администрации Дж. Байдена [Электронный ресурс] // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25. №3. С. 469–484. doi: 10.22363/2313-0660-2025-25-3-469-484. URL: https://journals.rudn.ru/international-relations/article/view/46265 (дата обращения: 11.11.2025).

4. Сокольщик Л.М., Сакаев В.Т., Галимуллин Э.З. Нелегальная иммиграция из Латинской Америки в контексте президентской кампании в США 2024 г.: эффекты поляризации [Электронный ресурс] // Международная аналитика. 2023. Т. 14, № 3. С. 106–126. https://doi.org/10.46272/2587-8476-2023-14-3-106-126

5. 2024 Report on the Cybersecurity Posture of the United States [Электронный ресурс] // White House. May 2024. URL: https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (accessed: 11.11.2025).

6. Bolgov R. The UN and Cybersecurity Policy of Latin American Countries [Электронный ресурс] // 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG). Buenos Aires, 2020. P. 259–263. DOI: 10.1109/ICEDEG48599.2020.9096798. URL: https://ieeexplore.ieee.org/abstract/document/9096798 (accessed: 11.11.2025)

7. Buzan B., Weaver O., Wide J. Security: a new framework for Analysis. London: Boulder, Lynne Rienner Publishers, 1998. [Электронный ресурс]. URL: https://www.academia.edu/39047709/Buzan_Waever_and_De_Wilde_1998_Security_A_New_Framework_For_Analysis (accessed: 11.11.2025)

8. Democracy Fund. Digital Democracy [Электронный ресурс] // Democracy Fund. URL: https://democracyfund.org/what-we-do/public-square/digital-democracy-portfolio/ (accessed: 11.11.2025)

9. Fact Sheet: 2023 DoD Cyber Strategy [Электронный ресурс] // Department of Defense. URL: https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF (accessed: 11.11.2025)

10. Global Partnership on Artificial Intelligence [Электронный ресурс] // Organisation for Economic Co-operation and Development. URL: https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html (accessed: 11.11.2025)

11. *Miao W., Xu J., Zhu H.* From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse (1994–2016) [Электронный ресурс] // Second International Handbook of Internet Research / ed. By J. Hunsinger, M. Allen, L. Klastrup. Dordrecht: Springer, 2019. URL: https://doi.org/10.1007/978-94-024-1202-4_61-1 (accessed: 11.11.2025)

12. National Cybersecurity Strategy [Электронный ресурс] // White House. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed: 11.11.2025).

13. United States International Cyberspace & Digital Policy Strategy [Электронный ресурс] // Department of State. URL: https://www.state.gov/release-of-united-states-international-cyberspace-and-digital-policy-strategy/ (accessed: 11.11.2025).

Секция В2

«Технологическая трансформация мировой экономики: искусственный интеллект, отрасли и новые модели управления»

Станислав Дмитриевич Казаченков,
старший преподаватель кафедры финансового и административного права,
Ростовский государственный экономический университет (РИНХ),
E-mail: kazachenkov94@mail.ru

Внучкова Ульяна Андреевна,
студентка группы ЮР-635,
Ростовский государственный экономический университет (РИНХ),
E-mail: ulianavnuchkova15@gmail.com

Карапетян Марина Седраковна,
студентка группы ЮР-635,
Ростовский государственный экономический университет (РИНХ),
E-mail: m.karapetyan555@yandex.ru

Stanislav D. Kazachenkov,
Senior Lecturer, Department of Financial and Administrative Law,
Rostov State University of Economics,
E-mail: kazachenkov94@mail.ru

Uliana A. Vnuchkova,
Student of Group YUR-635,
Rostov State University of Economics,
E-mail: ulianavnuchkova15@gmail.com

Marina S. Karapetyan,
Student of Group YUR-635,
Rostov State University of Economics,
E-mail: m.karapetyan555@yandex.ru

ЭТИКО-ПРАВОВЫЕ ВЫЗОВЫ И РЕГУЛЯТОРНЫЕ ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ФИНАНСОВО-ПРАВОВУЮ СФЕРУ РОССИИ

ETHICAL AND LEGAL CHALLENGES AND REGULATORY PERSPECTIVES OF ARTIFICIAL INTELLIGENCE IMPLEMENTATION IN THE FINANCIAL AND LEGAL SPHERE OF RUSSIA

Аннотация. В статье исследуются комплексные этико-правовые проблемы, возникающие в связи с интеграцией технологий искусственного интеллекта (ИИ) в финансово-правовую сферу на примере российской практики. Актуальность темы обусловлена активным внедрением алгоритмических систем Банком России, кредитными организациями и государственными органами. Новизна работы заключается в анализе коллизий между эффективностью ИИ и фундаментальными правовыми ценностями в специфических условиях российского правового поля, включая эксперимент по специальному регулированию в Москве. На примерах из практики (голосовые помощники, системы скоринга, биометрические данные) рассматриваются риски алгоритмической

дискриминации, проблемы установления виновности и перспективы формирования «умного» регулирования (RegTech и SupTech). Делается вывод о необходимости развития адаптивного правового поля, основанного на риск-ориентированном подходе.

Ключевые слова: искусственный интеллект, финансовая сфера, право, этика, алгоритмическое управление, дискриминация, подотчетность, регулирование.

Abstract. The article examines the complex ethical and legal challenges arising from the integration of artificial intelligence (AI) technologies into the financial and legal sphere, using Russian practice as an example. The relevance of the topic is driven by the active implementation of algorithmic systems by the Bank of Russia, credit institutions, and government agencies. The novelty of the work lies in the analysis of the conflicts between the efficiency of AI and fundamental legal values within the specific context of the Russian legal field, including the experiment on special regulation in Moscow. Using examples from practice (voice assistants, scoring systems, biometric data), the theses discuss the risks of algorithmic discrimination, problems of establishing liability, and the prospects for the formation of "smart" regulation (RegTech and SupTech). The conclusion is drawn on the necessity of developing an adaptive legal framework based on a risk-oriented approach.

Key words: artificial intelligence, financial sphere, law, ethics, algorithmic governance, discrimination, accountability, regulation.

Новая парадигма финансово-правовых отношений в России. Современная финансовая и правовая система России активно интегрирует технологии искусственного интеллекта. В соответствии со Стратегией развития искусственного интеллекта в РФ, утверждённой Указом Президента № 490, государство стимулирует внедрение ИИ в приоритетных сферах, включая финансовые услуги и правоприменение [5]. Европейский Союз уже принял первый в мире комплексный акт об искусственном интеллекте, установивший обязательства для компаний, разрабатывающих и использующих системы ИИ [2]. Важнейшим шагом стало принятие Федерального закона, который установил правовые основы для экспериментального режима в Москве [6]. Алгоритмы используются для автоматического принятия кредитных решений, выявления мошеннических операций, анализа судебной практики и работы Единой биометрической системы. Данный процесс, с одной стороны, сулит значительный рост эффективности. С другой стороны, он порождает ряд фундаментальных этико-правовых вызовов, специфичных для российского контекста.

Основные этико-правовые вызовы в российском контексте.

1. Алгоритмическая предвзятость и «кредитный шлагбаум».

Одним из наиболее острых вызовов является проблема алгоритмической дискриминации, которая в России может усугубляться региональной и социально-экономической неоднородностью.

Практический кейс: Скоринговые системы российских банков. Многие крупные банки (например, Тинькофф, СберБанк) используют proprietary-алгоритмы для скоринга потенциальных заёмщиков. Риск заключается в том, что алгоритмы, обучаясь на данных по преимущественно урбанизированному населению, могут занижать скоринговый балл для жителей малых городов и сёл, не потому что они являются ненадёжными заёмщиками, а из-за недостаточного цифрового следа или иных косвенных признаков. Это создаёт эффект «кредитного шлагбаума» для целых регионов, нарушая принципы справедливости и равенства, закреплённые в Конституции РФ [3, с. 48]. Проблема усугубляется непрозрачностью этих систем для потребителей и регулятора [7].

2. Проблема «чёрного ящика» и оспаривание решений.

Непрозрачность алгоритмов вступает в противоречие с требованиями российского законодательства, в частности, с правом потребителя на обоснование и мотивированный отказ, предусмотренным Законом «О защите прав потребителей».

Практический кейс: Голосовые помощники и чат-боты. Например, служба Банка России по защите прав потребителей рассматривала жалобу клиента, которому голосовой помощник одного из банков отказал в реструктуризации кредита с невнятной формулировкой. Клиент не мог понять логику отказа и, соответственно, не мог представить аргументированную апелляцию. Это классический пример «эффекта чёрного ящика»: решение, влияющее на права гражданина, не поддаётся полноценному анализу и оспариванию [4]. Федеральный закон № 123-ФЗ частично адресует эту проблему в рамках эксперимента в Москве, устанавливая особые условия обработки данных и тестирования ИИ, однако эта практика ещё не стала системной для всей страны [6].

3. Вопросы ответственности при использовании ИИ госорганами.

Использование ИИ в публично-правовой сфере ставит острые вопросы о распределении ответственности между разработчиком, оператором и государством.

Практический кейс: Системы видеоаналитики и автоматического выявления правонарушений. В Москве, в рамках действия Федерального закона № 123-ФЗ, широко внедрены системы распознавания лиц и видеоаналитики, которые, например, используются для автоматического выставления штрафов за нарушение ПДД. Хотя окончательное решение формально принимает инспектор, он де-факто полагается на данные алгоритма. В случае ошибки распознавания (например, штраф пришёл на автомобиль, которого не было в указанном месте) бремя доказывания своей невиновности ложится на гражданина. Это

переворачивает с ног на голову презумпцию невиновности и ставит вопрос: кто несёт ответственность за убытки, понесённые из-за ошибки алгоритма – городские власти, компания-разработчик или оба вместе?

4. Конфиденциальность данных и Единая биометрическая система (ЕБС)

Масштабный сбор биометрических данных для удалённой идентификации в финансовой сфере создаёт уникальные риски.

Практический кейс: Единая биометрическая система (ЕБС). Использование ЕБС банками для удалённого открытия счетов и получения кредитов – это прорыв в области цифровизации. Однако концентрация таких чувствительных данных в единой системе создаёт колоссальный риск в случае утечки. Федеральный закон № 123-ФЗ предоставляет Москве особые полномочия по формированию региональных составов данных, что является примером попытки структурировать этот процесс [6]. Тем не менее, возникают этические вопросы о возможности использования биометрии не только для идентификации, но и для поведенческого анализа (анализ эмоций по голосу или изображению) с целью оценки надёжности клиента. Правовых рамок для такого использования в России сегодня практически не существует, что создаёт правовой вакуум и потенциальную угрозу приватности [8].

Перспективы регулирования и этико-правовые стандарты в РФ.

1. Формирование «умного» регулирования (RegTech и SupTech).

Банк России является одним из лидеров во внедрении SupTech. Регулятор активно развивает Аналитический центр мониторинга и риск-ориентированного надзора (ЦМРН), который использует технологии Big Data и AI для анализа информации от кредитных организаций [1]. Это позволяет переходить от выборочных проверок к непрерывному мониторингу финансового сектора и проактивному выявлению рисков. Эксперимент по Федеральному закону № 123-ФЗ служит важным полигоном для отработки подобных подходов в городском хозяйстве.

2. Принципы «объяснимого ИИ» (XAI) и этические кодексы.

В России идёт активная дискуссия о необходимости разработки этических норм для ИИ. Альфа-Банк, Сбер и другие крупные игроки публично заявляют о разработке внутренних этических принципов использования ИИ [3]. На государственном уровне также обсуждается проект «Кодекса этики в сфере искусственного интеллекта», который, среди прочего, может закрепить принципы прозрачности и подотчётности алгоритмов, используемых в социально значимых сферах, включая финансы. Опыт, полученный в Москве в рамках закона № 123-ФЗ, может быть использован для выработки этих общенациональных стандартов.

3. Внедрение риск-ориентированного подхода через экспериментальные правовые режимы.

Ключевым инструментом для России становится Федеральный закон № 123-ФЗ, так как он позволяет создавать «регуляторные песочницы» для тестирования инновационных решений, в том числе в финансовой сфере, в условиях ослабленного регулирования, но с обязательным пост-анализом рисков и последствий. Это позволяет апробировать риск-ориентированный подход на практике и масштабировать успешные кейсы на всю страну.

Заключение. Интеграция искусственного интеллекта в финансово-правовую сферу России – это динамичный процесс, сопровождающийся специфическими вызовами: от рисков региональной дискриминации в скоринге до проблем оспаривания решений, принятых с участием ИИ госорганами. Федеральный закон № 123-ФЗ представляет собой важнейший первый шаг в создании адаптивной регуляторной среды, однако его действие ограничено Москвой и отдельными аспектами. Преодоление этих вызовов требует не простого копирования зарубежных регуляторных моделей, а выработки собственного пути, учитывающего особенности национальной правовой системы и социально-экономического ландшафта. Успех будет зависеть от скоординированного развития «умного» надзора со стороны Банка России, внедрения этических принципов на уровне компаний, формирования зрелого публичного дискурса о пределах и возможностях доверия к алгоритмам и от масштабирования успешного опыта экспериментальных правовых режимов на всю территорию РФ.

Список источников и литературы:

10. Банк России. Надзор за участниками финансового рынка с использованием технологий искусственного интеллекта [Электронный ресурс] // Вестник Банка России. – 2023. – № 15. – С. 12–25. URL: https://cbr.ru/Content/Document/File/... (дата обращения: 04.11.2025).

11. Европейский акт об искусственном интеллекте (Artificial Intelligence Act) [Электронный ресурс] // Future of Life Institute. URL: https://artificialintelligenceact.eu/ (дата обращения: 04.11.2025).

12. Кашкин С. Ю., Четвериков А. О. Право в эпоху цифровых технологий: новые вызовы и перспективы // Журнал зарубежного законодательства и сравнительного правоведения. – 2020. – № 5. – С. 44–52.

13. Таллиус Д. В. Искусственный интеллект и проблема ответственности в гражданском праве // Закон. – 2021. – № 3. – С. 25–35.

14. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 04.11.2025).

15. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ (ред. от 08 августа 2024 г.) «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве, об особенностях обработки персональных данных при формировании региональных составов данных и предоставления доступа к региональным составам данных и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» [Электронный ресурс] // КонсультантПлюс.
URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=499813&dst=100001 (дата обращения: 04.11.2025).

16. O'Neil, C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. – Crown Publishing Group, 2016. – 259 p.

17. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. – PublicAffairs, 2019. – 691 p.

Махнев Никита Дмитриевич,
студент 2-го курса обучения,
Филиал АлтГУ в г. Бийске
E-mail: manikita41@gmail.com

Пароваткина Дарья Ивановна,
студент 2-го курса обучения
Филиал АлтГУ в г. Бийске
E-mail: dasha2005parov@gmail.com

Фурсова Татьяна Григорьевна,
к.э.н., доцент,
Филиал АлтГУ в г. Бийске
E-mail: 89137104139@mail.ru

Makhnev Nikita Dmitrievich,
2nd year student,
AltSU Branch in Biysk
E-mail: manikita41@gmail.com

Daria Ivanovna Parovatkina,
2nd year student,
AltSU Branch in Biysk
E-mail: dasha2005parov@gmail.com

Fursova Tatyana Grigorievna,
Ph.D in Economics, Associate Professor,
AltSU Branch in Biysk
E-mail: 89137104139@mail.ru

ГЕОСЕРВИСЫ КАК ИНСТРУМЕНТ РАЗРАБОТКИ И ПРОДВИЖЕНИЯ БРЕНДИНГОВОГО ТУРИСТИЧЕСКОГО МАРШРУТА (НА ПРИМЕРЕ «КАТУНСКОЙ ТРОПЫ» В АЛТАЙСКОМ КРАЕ)

GEOSERVICES AS A TOOL FOR DEVELOPING AND PROMOTING A BRANDED TOURIST ROUTE (USING THE EXAMPLE OF THE «KATUN TRAIL» IN THE ALTAI REGION)

Аннотация. Геосервисы становятся ключевым инструментом проектирования и продвижения туристических маршрутов, одновременно предъявляя требования к точности, актуальности и безопасности, в условиях цифровизации туристской отрасли. Практическая значимость – в ходе полевых исследований с GPS-трекингом для обеспечения цифровой безопасности и минимизации навигационных ошибок был разработан брендинговый

туристический маршрут «Катунская тропа» и созданы рекомендации по его интеграции в популярный геосервис 2ГИС, а также публикацию GPS-трека, ключевых точек, фотографий и дополнительных маркеров. Эти действия являются важным элементом повышения цифровой доступности, безопасности и устойчивого продвижения маршрута на территории Алтайского края.

Чтобы сформировать достоверные пространственные данные и снизить риски, связанные с некорректной навигацией пользователей, которые являются одними из факторов цифровой безопасности туристов были проведены полевые исследования маршрута с помощью GPS-трекинга.

Ключевые слова: геосервис, туристический маршрут, цифровизация, брендинговый маршрут, Катунская тропа, 2ГИС, GPS-трек, интеграция, пространственные данные, полевые исследования, навигация, цифровая доступность, безопасность, продвижение, Алтайский край, технологическая карта, паспорт маршрута, сравнительный анализ, рекомендации.

Abstract. Geoservices are becoming a key tool for designing and promoting tourist routes, while at the same time imposing requirements for accuracy, relevance, and security in the context of the digitalization of the tourism industry. Practical significance: a branded tourist route, “Katun Trail,” has been developed, and recommendations have been made for its integration into the popular geoservice 2GIS, as well as the publication of GPS tracks, key points, photos, and additional markers. These actions are an important element in improving digital accessibility, safety, and sustainable promotion of the Altai Territory.

In order to generate reliable spatial data and reduce the risks associated with incorrect user navigation, which are among the factors affecting the digital safety of tourists, field studies of the route were conducted using GPS tracking.

Key words: geoservice, tourist route, digitalization, branding route, Katun Trail, 2GIS, GPS track, integration, spatial data, field research, navigation, digital accessibility, safety, promotion, Altai Krai, technology map, route passport, comparative analysis, recommendations.

Актуальность исследования. В условиях цифровизации около 97% людей интернет-пользователей России ищут что-либо через геосервисы (Яндекс.Карты, 2ГИС, Google Maps) хотя бы раз в месяц [1]. Для брендовых туристических маршрутов, являющихся конкурентным преимуществом регионов, интеграция в эти платформы стала необходимостью. Это позволяет не только повысить узнаваемость, но и обеспечить безопасность и комфорт туристов за счет предоставления актуальной информации. Цель исследования − разработать брендинговый туристический маршрут «Катунская тропа» и

обосновать комплекс мер по его интеграции в популярные геосервисы. Для этого были решены следующие задачи:

1) Систематизировать теоретические аспекты использования геосервисов на всех этапах жизненного цикла туристического маршрута, от проектирования до продвижения.

2) Провести полевые исследования природных особенностей берега реки Катунь в окрестностях села Сростки с применением GPS-трекинга для точной пространственной привязки маршрута и ключевых мест.

3) Для внесения достоверной информации в карточку геосервиса определить ключевые параметры маршрута и разработать его документацию (технологическая карта и паспорт).

4) На основе сравнительного анализа определить целевые геоплатформы и разработать практические рекомендации по наполнению их карточки маршрута «Катунская тропа».

Методология и методы исследования. В работе применялись методы системного анализа, сравнительный анализ функционала геосервисов (Яндекс.Карты, 2ГИС, Google Maps), а также полевые исследования с использованием GPS-навигации для построения трека.

Основные результаты. На основе полевых исследований создан линейный маршрут «Катунская тропа», протяженностью 8-10 км вдоль берега реки Катунь. Его ключевые параметры (координаты старта и финиша, точек показа, перепады высот) определены с использованием геоданных. Приоритетной платформой для продвижения была выбрана 2ГИС, так как данный геосервис пользуется популярностью в регионе и имеет специальный «туристический слой». Помимо этого, 2ГИС имеет успешный региональный опыт по нанесению экологических троп при поддержке Сбера [2].

Для эффективной интеграции маршрута был создан детальный план наполнения карточки, включающий в себя размещение GPS-трека с точной геометрией пути, публикации детальной информации о маршруте, добавления фотографий и маркеров (для навигации и отображения ключевых точек), мониторинга отзывов для улучшения тропы.

Заключение. Интеграция брендингового маршрута «Катунская тропа» в геосервис 2ГИС является ключевым элементом его жизненного цикла. Данный подход обеспечивает взаимосвязь между обустройством тропы и ее цифровым представлением, что влияет на увеличение туристского потока, развитию территории и повышению узнаваемости туристического потенциала Бийского района.

Список источников и литературы:

1. Аудитория геосервисов: кто пользуется онлайн-картами и навигацией [Электронный ресурс] // Yandex. URL: https://yandex.ru/adv/solutions/analytics/auditoriya-geoservisov-kto-polzuetsya-onlajn-kartami-i-navigaciej (дата обращения: 19.10.2025).

2. Новость: В Алтайском крае при поддержке Сбера на карты 2ГИС нанесли экологические тропы [Электронный ресурс] // ALTAPRESS. URL: https://altapress.ru/zhizn/story/v-altayskom-krae-pri-podderzhke-sbera-na-karti-gis-nanesli-ekologicheskie-tropi-322643 (дата обращения: 23.10.2025).

Ирина Андреевна Плехова, Любовь Владимировна Чашкина,
студентки 3 курса,
Шадринский финансово –экономический колледж филиал
Федерального государственного образовательного бюджетного учреждения
высшего образования
«Финансовый университет при Правительстве Российской Федерации»,
E-mail: irina233plehova@yandex.ru; 1may0820@mail.ru

Irina A. Plekhova, Lyubov V. Chashkina,
3rd year students,
Shadrinsky Financial and Economic College, a branch of the Federal State Educational
Budgetary Institution of Higher Education "Financial University under the Government of the
Russian Federation",
E-mail: irina233plehova@yandex.ru; 1may0820@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БУДУЩЕЕ ПРОФЕССИЙ: ВЛИЯНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РЫНОК ТРУДА И ПОТРЕБНОСТИ В КОМПЕТЕНЦИЯХ СОТРУДНИКОВ

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF PROFESSIONS: THE IMPACT OF ARTIFICIAL INTELLIGENCE TECHNOLOGY ON THE LABOR MARKET AND THE NEED FOR EMPLOYEES' COMPETENCIES

Аннотация. Авторы исследуют трансформационное воздействие технологий искусственного интеллекта (ИИ), в частности генеративных моделей, на глобальный рынок труда. Анализируют переход от автоматизации рутинных задач к изменению содержания интеллектуального труда. Авторы рассматривают две ключевые парадигмы: замещение человеческих функций и усиление человеческих возможностей. Основное внимание уделяется изменению структуры компетенций, необходимых для сохранения конкурентоспособности сотрудников в условиях стремительной цифровизации. Делается вывод о необходимости системной перестройки образовательных и корпоративных систем обучения.

Abstract. The authors explore the transformative impact of artificial intelligence (AI) technologies, particularly generative models, on the global labor market. They analyze the shift from automation of routine tasks to changes in the content of intellectual labor. The authors examine two key paradigms: the replacement of human functions and the enhancement of human capabilities (Human-AI collaboration). The focus is on the evolving structure of competencies required to maintain the competitiveness of employees in the face of rapid digitalization. The

authors conclude that there is a need for a systemic overhaul of educational and corporate training systems.

Ключевые слова: искусственный интеллект, генеративный ИИ, рынок труда, компетенции будущего, автоматизация знаний, человеко-машинное взаимодействие, непрерывное обучение.

Key words: artificial intelligence, generative AI, labor market, future competencies, knowledge automation, human-machine interaction, and continuous learning.

Современный этап развития технологий искусственного интеллекта, ознаменованный появлением мощных генеративных моделей и больших языковых моделей, выводит дискуссию о будущем труда на качественно новый уровень. Если предыдущие волны автоматизации затрагивали в основном рутинный физический и конвейерный труд, то сегодня ИИ демонстрирует способность выполнять комплексные когнитивные задачи: создание контента, анализ кода и поддержку принятия решений. Это ставит под вопрос устойчивость не только рабочих мест, но и многовековой монополии человека на интеллектуальный труд.

Современный ландшафт воздействия ИИ на профессии: от автоматизации к парадигме «усиления». Влияние ИИ на профессиональную деятельность стало более комплексным. Исследовательские организации выделяют несколько сценариев взаимодействия человека и ИИ, основной из них – автоматизация задач, а не профессий. Согласно докладам Всемирного экономического форума 2023 г. [5] и McKinsey [5], полное исчезновение профессий под натиском ИИ маловероятно в обозримом будущем. Однако значительная часть задач в рамках большинства профессий подвержена автоматизации. Речь идет в первую очередь о задачах, связанных с обработкой информации: поиск и синтез данных, составление первичных отчетов, классификация, базовый анализ и коммуникация по стандартным запросам. Это затрагивает сферы юриспруденции, маркетинга, программирования, образования и финансов.

Еще одним сценарием взаимодействия человека и ИИ выступает парадигма «усиления». На смену нормативу о замещении приходит концепция «усиления» человеческих способностей с помощью ИИ. В этой модели ИИ выступает как интеллектуальный ассистент или «когнитивный экзоскелет», который берет на себя рутинные интеллектуальные операции, высвобождая время человека для задач более высокого порядка. Например, архитектор использует ИИ для генерации эскизов по текстовому описанию, сосредотачиваясь на концептуальном проектировании и работе с клиентом. Врач использует ИИ-систему для анализа медицинских изображений, что

позволяет ему уделить больше времени комплексной диагностике и общению с пациентом. Это приводит не к исчезновению профессии, а к трансформации ее ядра и повышению производительности.

Возникновение новых профессиональных ролей и экосистем. Технологии ИИ порождают спрос на новые, ранее не существовавшие специальности, а также радикально меняют содержание существующих, например, *п*рямые профессии в сфере ИИ. Продолжает расти спрос на специалистов, создающих и обслуживающих системы ИИ: инженеры по машинному обучению, разработчики моделей, специалисты по проектированию эффективных запросов к ИИ, эксперты по AI-безопасности и этике. Примечательно, что сама экосистема ИИ создает рабочие места для его же развития.

Наиболее значительный тренд – рост спроса на гибридных специалистов, которые сочетают глубокие предметные знания с навыками применения ИИ-инструментов в своей области (так называемых специалистов «с двумя шляпами»). Это приводит к появлению таких ролей, как:

– ИИ-стратег в бизнесе – специалист, который определяет, где и как внедрить ИИ для решения ключевых бизнес-задач;

– цифровой лингвист/антрополог – эксперт, который работает с языковыми моделями, улучшая их понимание контекста и специфики предметной области;

– специалист по взаимодействию человека и ИИ проектирует интерфейсы и процессы, обеспечивающие эффективную коллаборацию между человеком и алгоритмом.

Трансформация компетенций: запрос на «мягкие» и «надпрофессиональные» навыки. Сдвиг в содержании труда диктует необходимость кардинального обновления модели компетенций. Технические навыки устаревают с беспрецедентной скоростью, в то время как универсальные когнитивные и социальные навыки выходят на первый план. Способность критически оценивать выводы, сгенерированные ИИ, проверять их на достоверность, выявлять скрытые смещения и интегрировать их в более широкий стратегический контекст становится ключевой. ИИ предоставляет данные и гипотезы, но ответственность за верификацию и окончательное решение остается за человеком.

В условиях, когда ИИ может генерировать стандартные решения, ценность способности человека формулировать принципиально новые вопросы, создавать оригинальные продукты и выдвигать неочевидные идеи резко возрастает. Креативность становится не факультативным, а базовым навыком. Навыки межличностного общения, управления коллективами, убеждения и проявления эмпатии остаются областью, где человек сохраняет безусловное преимущество. В автоматизированном мире «человеческое

лицо» бизнеса и способность выстраивать доверительные отношения становятся критически важными активами.

Немаловажное значение имеют цифровая и ИИ-грамотность. При этом речь идет не о необходимости всем становиться программистами, а о понимании базовых принципов работы ИИ, его возможностей, ограничений и рисков. Сотрудник должен уметь эффективно формулировать запросы к ИИ-системам и интерпретировать их ответы.

Адаптивность и готовность к непрерывному обучению, способность к быстрой перестройке, освоению новых инструментов и парадигм становятся основными навыками выживания на рынке труда. Карьера превращается из восхождения по вертикальной лестнице в серию горизонтальных переходов и постоянного обновления знаний.

Ключевыми вызовами ближайшего пятилетия станут:

1. Преодоление структурного разрыва в навыках – стремительное расхождение между компетенциями, которые формирует традиционная система образования, и реальными потребностями экономики, основанной на коллаборации с ИИ.
2. Внедрение моделей непрерывного обучения – необходимость создания гибких и доступных систем переобучения и повышения квалификации как на национальном уровне, так и внутри компаний.
3. Управление социальными последствиями – риски роста неравенства из-за неравного доступа к возможностям переобучения и цифровым инфраструктурам.

Заключение. Технологии ИИ, особенно в их генеративной ипостаси, выступают в роли мощного катализатора структурной перестройки глобального рынка труда. Основной тренд заключается не в массовом замещении человека машиной, а в глубокой трансформации профессиональных ландшафтов, где рутинные когнитивные задачи переходят к алгоритмам, а человеческий потенциал переориентируется на деятельность, требующую креативности, критического мышления, эмоционального интеллекта и стратегического видения. Успешная адаптация к новым реалиям требует скоординированных действий правительств, образовательных учреждений и бизнеса. Будущее труда принадлежит не тем, кто будет конкурировать с ИИ, а тем, кто научится с ним эффективно сотрудничать, используя машину для усиления своих уникальных человеческих качеств. Инвестиции в развитие «мягких» навыков и создание культуры непрерывного обучения становятся главным стратегическим приоритетом для обеспечения конкурентоспособности как отдельных сотрудников, так и целых экономик.

Список источников и литературы:

1. Интеллектуальные роботы, киборги, генетически усовершенствованные индивиды, химеры: будущее и задачи права (И.А.Филипова, 2024) [Электронный ресурс] // URL: https://cyberleninka.ru/article/n/intellektualnye-roboty-kiborgi-geneticheski-usovershenstvovannye-individy-himery-buduschee-i-zadachi-prava?ysclid=mhtazf5fp6221885115 (дата обращения: 08.11.2025).
2. Acemoglu, D., & Restrepo, P. (2022). Tasks, Automation, and the Rise in U.S. Wage Inequality [Электронный ресурс] // Econometrica, 90 (5). URL: https://economics.mit.edu/sites/default/files/2022-10/Tasks%20Automation%20and%20the%20Rise%20in%20US%20Wage%20Inequality.pdf (дата обращения: 08.11.2025).
3. Brynjolfsson, E., & McAfee, A. (2023). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies (2nd ed.) [Электронный ресурс] // W. W. Norton & Company. URL: https://archive.org/details/secondmachineage0000bryn/page/n5/mode/2up (дата обращения: 08.11.2025).
4. McKinsey Global Institute. (2023) [Электронный ресурс] // Generative AI and the future of work in America. URL: https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america (дата обращения: 08.11.2025).
5. World Economic Forum. (2023) [Электронный ресурс] // The Future of Jobs Report 2023. URL: https://newsletter.radensa.ru/wp-content/uploads/2023/11/WEF_Future_of_Jobs_2023.pdf?ysclid=mhrqk4rigs766197163 (дата обращения: 08.11.2025).

Сюй Жуйлинь,
аспирант Кафедры сравнительной политологии
ФГСН РУДН
E-mail: xuruilin@yandex.ru

Xu Ruilin,
Ph.D student in Department of Comparative Politics,
Faculty of Humanities and Social Sciences,
RUDN University
E-mail: xuruilin@yandex.ru

ВЫЗОВЫ ДЛЯ РОССИЙСКО-КИТАЙСКОГО СОТРУДНИЧЕСТВА В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ

CHALLENGES FOR RUSSIAN-CHINESE COOPERATION IN THE DIGITAL ECONOMY

Аннотация. На фоне углубления глобальной экономической интеграции и стремительного развития цифровых технологий цифровая торговля превратилась в новый двигатель международного экономического сотрудничества и развития. Партнёрство между Китаем и Россией в этой сфере не только определяет будущую траекторию развития их экономик, но и оказывает существенное влияние на процветание глобальной цифровой торговли. Вместе с тем, в процессе сотрудничества обе стороны сталкиваются с комплексом внутренних и внешних вызовов, включая различия в технологиях и стандартах, дефицит кадров в области цифровой торговли, необходимость совершенствования систем кибербезопасности, последствия международных санкций, потенциальные риски, связанные с ухудшением информационного фона, и конкуренцию в сфере регулирования цифрового пространства. В этой связи Китаю и России следует активизировать политический диалог и координацию, повышать уровень кибербезопасности и совместно способствовать устойчивому развитию цифровой торговли для достижения взаимовыгодных целей.

Ключевые слова: Российско-китайские сотрудничства, цифровая экономика, санкции, финансовое сотрудничество.

Abstract. Against the backdrop of deepening global economic integration and the rapid development of digital technologies, digital trade has become a new engine for international economic cooperation and development. The partnership between China and Russia in this sphere not only determines the future trajectory of their economic development but also significantly influences the prosperity of global digital trade. However, in the process of cooperation, both sides face a complex set of internal and external challenges, including differences in technologies and standards, a shortage of personnel in digital trade, the need to improve cybersecurity systems, the consequences of international sanctions, potential risks associated with a deteriorating information environment, and competition in the realm of digital space regulation. In this regard, China and Russia should intensify political dialogue and coordination, enhance the level of cybersecurity, and jointly promote the sustainable development of digital trade to achieve mutually beneficial goals.

Key words: Russian-Chinese Cooperation, digital economy, sanctions, financial cooperation.

Под влиянием процессов глобализации и информатизации цифровая экономика стала новым катализатором мирового экономического роста. В данном контексте для Китая и России как значимых игроков в глобальной экономике и стратегических партнёров вопрос углубления сотрудничества в сфере цифровой экономики с целью достижения синергетического эффекта приобрел характер совместной стратегической задачи.

Внутренние вызовы для российско-китайского сотрудничества в сфере цифровой экономики. В условиях ускоряющейся глобальной цифровой трансформации сотрудничество между Китаем и Россией в области цифровой экономики стало важной опорой их стратегического взаимодействия. Однако по мере углубления этого сотрудничества всё отчётливее проявляется комплекс внутренних структурных вызовов, сдерживающих раскрытие его полного потенциала. Эти вызовы проявляются не только в различиях технологических и стандартизационных систем, но и в структурном дефиците кадровых ресурсов, а также в уровне развития систем кибербезопасности.

1. Различия в технологиях и стандартах: существуют различия в определениях, классификации и системах оценки цифровой экономики. Китай придерживается более широкого подхода, Россия фокусируется на интеграции с традиционными отраслями. Это приводит к проблемам интероперабельности, росту издержек и сегментации рынков [8].

2. Дефицит кадров в сфере цифровой торговли: Китай испытывает значительный дефицит специалистов (разрыв в 6 млн человек). Конфликт на Украине усугубил «утечку умов» из России (не менее 100 тыс. ИТ-специалистов в 2022 г.), что подрывает инновационный потенциал и создает угрозы безопасности [3].

3. Необходимость совершенствования системы кибербезопасности: Учащающиеся инциденты (утечки данных, мошенничество, контрафактная продукция на кросс-бордер платформах) и различия в законодательстве о защите данных и кибербезопасности увеличивают сложность трансграничной торговли и требуют усиления координации [12].

Внешние вызовы для российско-китайского сотрудничества в сфере цифровой экономики. В контексте СВО сотрудничество между Китаем и Россией в сфере цифровой экономики сталкивается с беспрецедентной сложностью и неопределенностью, внешнее давление становится важным фактором, влияющим на пути сотрудничества двух сторон, и порождает ряд вызовов, требующих решения.

1. Влияние международных санкций: санкции против России, включая ограничения на экспорт высоких технологий и доступ к международным цифровым платформам, напрямую повлияли на ключевые области, такие как ИИ, ИВ и 5G, приводя к снижению инвестиций в НИОКР и задержкам проектов [10]. Вторичные санкции создают риски для китайских компаний, ограничивая глубину сотрудничества, как показал пример Alibaba [1].

2. Потенциальные риски ухудшения информационной среды: ограничения для российских медиа на глобальных платформах подрывают коммуникационные возможности России, что в долгосрочной перспективе может негативно сказаться на взаимном доверии и увеличить риски для экономического сотрудничества, включая инвестиции и технологический обмен [7].

3. Соперничество в сфере регулирования цифрового пространства: США создают эксклюзивные технологические союзы и продвигают свои шаблоны правил цифровой торговли через региональные соглашения, пытаясь исключить Китай и Россию. Это вынуждает две страны искать баланс между адаптацией и продвижением собственных нормативных подходов, рискуя занять пассивную позицию [13].

Направления развития российско-китайского сотрудничества в сфере цифровой экономики. Сталкиваясь с существующими вызовами, Китаю и России следует, придерживаясь принципов открытости, взаимной выгоды и обоюдного выигрыша, использовать предоставленные историей возможности для углубления сотрудничества в области цифровой экономики, совместного исследования новых моделей инновационного развития, а также содействия процветанию и устойчивому развитию цифровой экономики двух стран и всего мира.

Конкретные направления и меры включают:

1. Модернизация платформ сотрудничества: северо-восточным регионам Китая целесообразно внедрить льготную политику для цифровых компаний, создать промышленные кластеры и модернизировать традиционные платформы сотрудничества, используя географическую близость к России [6].

2. Расширение сфер сотрудничества: необходимо активизировать обмен техническими специалистами с промышленно развитыми регионами России, совершенствовать транспортную инфраструктуру и развивать торговлю услугами для расширения границ цифровой торговли.

3. Усиление кадрового обмена и сотрудничества: следует создать комплексный механизм сотрудничества, включая совместные исследовательские институты, учебно-производственные базы, программы обмена студентами, семинары и тренинги для подготовки кадров с международным кругозором [9]. Развитие ИИ создает благоприятную среду для этого.

4. Укрепление защиты кибербезопасности: на базовом уровне необходимо усиливать защиту и популяризировать знания о кибербезопасности. На техническом уровне требуется классифицировать данные, обеспечивать контроль над критически важными данными, обновлять технологические резервы и разрабатывать планы действий в ЧС.

Заключение. Несмотря на комплекс внутренних и внешних вызовов, российско-китайское сотрудничество в сфере цифровой экономики обладает значительным потенциалом. Формирование более тесного партнёрства, модернизация платформ, расширение областей взаимодействия, активизация кадрового обмена и укрепление кибербезопасности позволят сторонам эффективно преодолеть существующие препятствия, достичь синергетического развития и внести вклад в глобальное цифровое управление.

Список источников и литературы:

1. Диалог.UA. Удар в спину：Alibaba перестала принимать рубли и поставлять товары в Россию , 2024-06-02. Диалог. UA. URL: https : //www.dialog.ua/russia/295772_1716987003 (дата обращения: 11.12.2025).

2. Зубенко Вячеслав Васильевич，Зубенко Вера Андреевна，Сунь Юаньюе Российско-китайское сотрудничество в области цифровой экономики［J］.Гуманитарные науки. Вестник Финансового университета. 2023. №3. С.86-93.

3. Интерфакс. Глава Минцифры сообщил，что порядка 100 тыс . айтишников покинули РФ в этом год, 2024-03-20. Интерфакс. URL: https : //www.interfax.ru/russia/877771 (дата обращения: 11.12.2025).

4. Комлева，С. А. Развитие китайско - российского сотрудничества в области цифровой экономики. Цифровая экономика глазами студентов : материалы Международной научной конференции，Казань，12 мая 2023 года. – Казань：ИП Сагиев А.Р.，2023.–с. 122-125.

5. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы. Указ Президента РФ от 9 мая 2017 г. № 203.

6. 曹曦文,杨慧瀛.深化中俄数字贸易合作[J].中国外资,2024,(07):41-43.

7. 邓伟志 . 社会学辞典. 上海 : 上海辞书出版社，2009 : 525.

8. 高际香 . 俄罗斯数字经济发展与数字化转型. 欧亚经济，2020（1）: 21-37.

9. 胡明 . 中俄数字经济合作 : 现状、挑战与推进战略 . 东北亚论坛 ,2025,34(01):65-83+128.DOI:10.13654/j.cnki.naf.2025.01.005.

10. 蓝庆新，汪春雨，尼古拉 . 俄罗斯数字经济发展与中俄数字经济合作面临的新挑战. 东北亚论坛，2022（5）: 111-126.

11. 刘军梅，徐浩然，余宇轩 . 俄乌冲突背景下的俄罗斯数字经济 : 制裁冲击与战略调整. 俄罗斯研究，2023（5）: 23-46.

12. 刘璐琪,王秋兰.中俄数字贸易合作深化 : 现状、挑战与对策建议[J].商业经济 ,2025,(07):98-101.DOI:10.19905/j.cnki.syjj1982.2025.07.002.

13. 数字贸易协议不应成为美国制衡中国新工具，中美聚焦，2021.09.30，https://cn.chinausfocus.com/finance-economy/20210930/42412.html

Андрей Владимирович Уфимцев,
студент 1 курса магистратуры Томского политехнического университета,
E-mail: avu34@tpu.ru

Andrey V. Ufimtsev,
1st year master's student of Tomsk Polytechnic University
E-mail: avu34@tpu.ru

ЭКОНОМИКО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ СИСТЕМ УСОВЕРШЕНСТВОВАННОГО УПРАВЛЕНИЯ В НЕФТЕГАЗОВОЙ ОТРАСЛИ

ECONOMIC AND MANAGERIAL ASPECTS OF THE IMPLEMENTATION OF ADVANCED CONTROL SYSTEMS IN THE OIL AND GAS INDUSTRY

Аннотация. В статье рассматриваются экономические и управленческие аспекты внедрения систем усовершенствованного управления на предприятиях нефтегазового комплекса. Проанализированы преимущества сервисной модели внедрения, сочетающей многопараметрическое управление и виртуальные анализаторы качества. Представлены результаты внедрения системы, демонстрирующие снижение эксплуатационных расходов и повышение управляемости производства. Особое внимание уделено вопросам информационной безопасности при реализации подобных проектов.

Ключевые слова: системы усовершенствованного управления, сервисная модель, виртуальные анализаторы, нефтегазовый комплекс, информационная безопасность.

Abstract. The article examines the economic and managerial aspects of the implementation of advanced control systems at oil and gas industry enterprises. The advantages of a service implementation model combining multiparameter control and virtual quality analyzers are analyzed. The results of the system implementation demonstrating the reduction of operating costs and improved production controllability are presented. Special attention is paid to information security issues in the implementation of such projects.

Key words: advanced control systems, service model, virtual analyzers, oil and gas industry, information security.

Современные вызовы, стоящие перед нефтегазовой отраслью, требуют новых подходов к управлению производственными активами. Жесткая конкуренция и волатильность рынка обуславливают необходимость постоянного поиска резервов для

снижения издержек и повышения гибкости управления. Одним из наиболее перспективных направлений является цифровая трансформация технологических процессов через внедрение интеллектуальных систем управления. Однако традиционный путь, связанный с крупными капитальными вложениями в оборудование и программное обеспечение, зачастую экономически нецелесообразен. В качестве альтернативы предлагается сервисная модель, основанная на применении методов математического анализа данных для построения систем усовершенствованного управления. Данный подход позволяет перераспределить финансовые потоки с капитальных на операционные расходы, получая при этом доступ к передовым технологиям оптимизации [1].

Описание технологического процесса и проблем управления. Объектом исследования выступила установка газоразделения и стабилизации конденсата, типичный технологический актив нефтегазового предприятия. Ключевой проблемой подобных установок является низкая эффективность систем автоматического регулирования, традиционно построенных на простых ПИД-алгоритмах. Эти системы не способны комплексно учитывать взаимовлияние множества технологических параметров, что приводит к устойчивым колебаниям режима, повышенному энергопотреблению и необходимости частого вмешательства оперативного персонала [2]. Такая ситуация порождает существенные операционные риски, увеличивает долю некондиционной продукции и снижает общую экономическую эффективность производства. Анализ исторических данных работы установки подтвердил недостаточную точность поддержания ключевых параметров, что напрямую влияло на себестоимость выпускаемой продукции.

Методология и разработанное решение. Разработанное решение представляет собой комплексную систему, интегрирующую виртуальный анализатор качества и многопараметрический прогнозирующий контроллер. Первым этапом стал регрессионный и корреляционный анализ исторических данных для выявления скрытых зависимостей между параметрами процесса [3]. Это позволило разработать высокоточную математическую модель виртуального анализатора, непрерывно в реальном времени рассчитывающего ключевые показатели качества продукции на основе данных стандартных приборов КИП. Использование методов, таких как радиальные базисные функции и фильтр Калмана, обеспечило модели адаптивность и устойчивость к мультиколлинеарности данных.

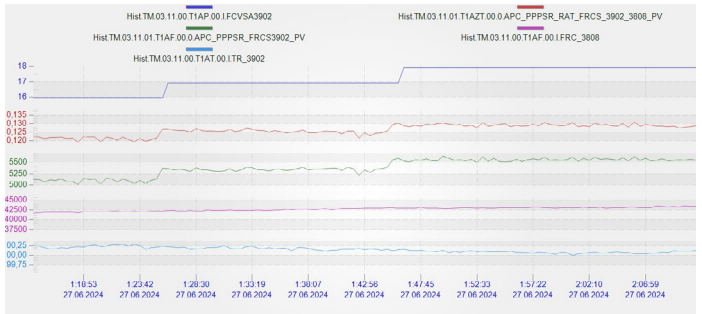


Рис. 1. Анализ трендовых групп параметров колонны газоразделения. Составлено автором

Основой для построения системы управления стало проведение планового пошагового теста, который, несмотря на временные отклонения от нормального режима, представлял собой стратегическую инвестицию в создание цифрового двойника технологического процесса. Полученные данные позволили построить точные динамические модели, описывающие реакцию контролируемых параметров на управляющие воздействия.

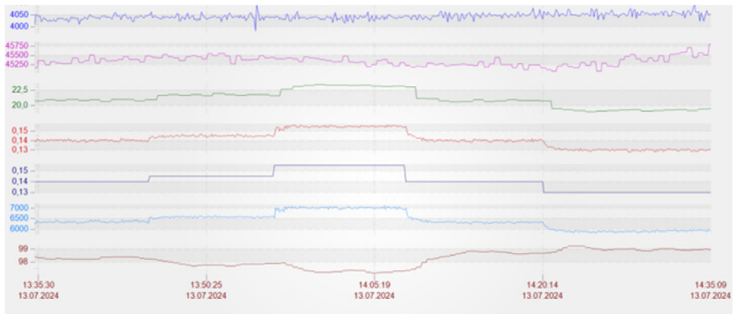


Рис. 2. Результат пошагового теста с колонны. Составлено автором

Принципиальным управленческим решением стал переход от регулирования по вторичным параметрам к управлению по фундаментальному параметру – тепловому потоку колонны [4]. Этот параметр интегрально учитывает множество факторов, что позволило кардинально повысить стабильность технологического процесса.

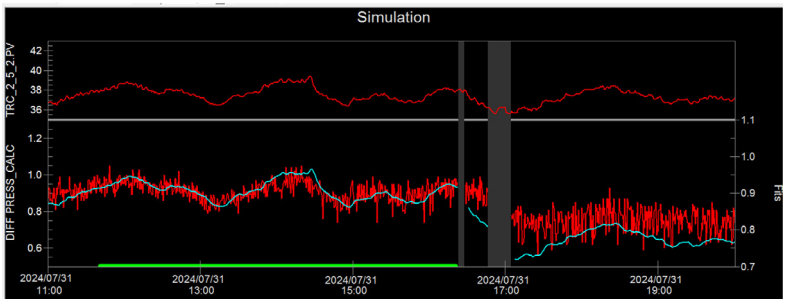


Рис. 3. Зависимость управляющего воздействия на основе теплового потока на температуру верха колонны. Составлено автором

Экономико-управленческое обоснование и результаты. Сравнительный анализ эффективности показал значительное превосходство многопараметрического контроллера над классическими системами. Быстродействие системы при регулировании уровня разделения сред повысилось на пятьдесят процентов, а при регулировании перепада давления – на тридцать два процента. Энергетические затраты на осуществление управления снизились на четырнадцать и двадцать один процент соответственно [5]. Эти технические улучшения имеют прямую экономическую интерпретацию. Повышение быстродействия напрямую снижает объем некондиционного продукта, производимого в переходных режимах. Снижение энергозатрат транслируется в прямое сокращение счетов за энергоносители.

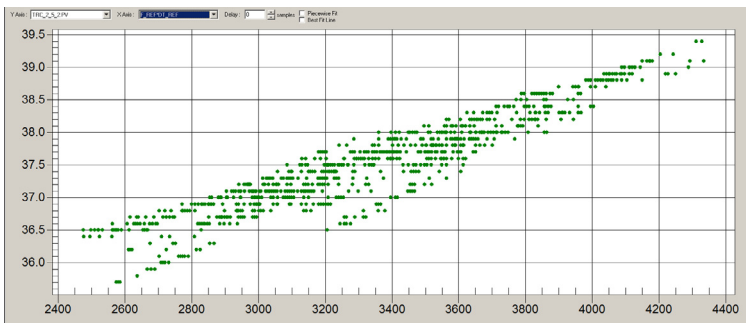


Рис. 4. Кросс-плот вероятностного распределения значений температуры верха колонны. Составлено автором

Суммарный экономический эффект от внедрения сервиса интеллектуального управления оценивается в диапазоне от двух до пяти процентов снижения операционных

расходов. Срок окупаемости проекта составляет от шести до восемнадцати месяцев в зависимости от масштаба производства. Основными источниками экономии являются снижение удельного расхода энергоносителей, увеличение выхода целевого продукта, сокращение потерь от брака, а также высвобождение персонала для решения более сложных аналитических задач. Таким образом, проект рассматривается не как операционная затрата, а как инвестиционная инициатива с быстрой окупаемостью и минимальными рисками.

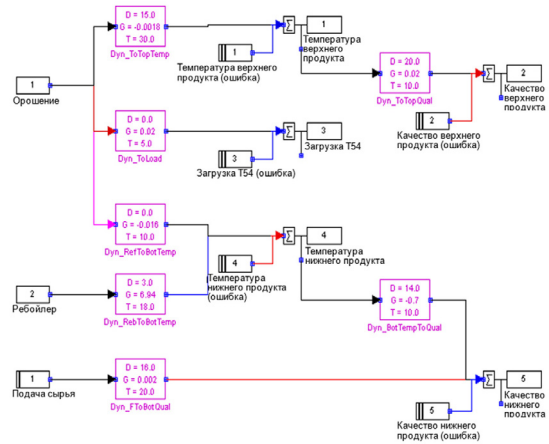


Рис. 5. Детализация параметров контроллера СУУТП. Составлено автором

Заключение. Проведенное исследование подтверждает, что внедрение систем усовершенствованного управления на основе глубокого математического анализа данных является мощным инструментом повышения операционной эффективности и конкурентоспособности нефтегазовых предприятий. Предложенная сервисная модель позволяет оптимально перераспределить финансовые и человеческие ресурсы, создавая устойчивый поток экономии и повышая рентабельность активов. С управленческой точки зрения, переход к проактивной оптимизации технологических процессов позволяет не только снизить текущие расходы, но и повысить прогнозируемость бизнес-показателей, что особенно ценно в условиях нестабильности рынков. Дальнейшее развитие проекта видится в тиражировании данной модели на другие технологические объекты и адаптации предложенных решений для смежных отраслей промышленности.

Список источников и литературы:

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

2. Марушак Г.М. Система автоматического управления процессом ректификации: пат. RU 2 176 149 C1. 2001.

3. Сидоров В.П. Цифровая трансформация промышленности. М.: ТехноПресс, 2023. 210 с.

4. Шумихин А.Г. Опыт разработки системы виртуального анализа показателей качества продуктов установок каталитического риформинга // Вестник Пермского национального исследовательского политехнического университета. 2017. № 2. С. 45–62.

5. Smith J. Intelligent Systems in Chemical Industry // Journal of Advanced Manufacturing. 2022. Vol. 15. P. 45–52.

Анастасия Олеговна Чернобривченко,
студент 3 курса магистратуры факультета
Международного энергетического бизнеса
РГУ нефти и газа (НИУ) имени И.М. Губкина
E-mail: chernobrivchenko.ana@yandex.ru

Anastasiia O. Chernobrivchenko,
Third-year Master's student
in International Energy Business
National University of Oil and Gas
«Gubkin University»
E-mail: chernobrivchenko.ana@yandex.ru

РОЛЬ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В РАЗВИТИИ НЕФТЕГАЗОВОЙ ОТРАСЛИ НА ПРИМЕРЕ КОМПАНИИ BRITISH PETROLEUM

IMPACT OF DIGITAL TRANSFORMATION ON THE OIL AND GAS INDUSTRY: BRITISH PETROLEUM EXPERIENCE

Аннотация. Проведен анализ роли цифровых инноваций в развитии энергетической отрасли на примере компании British Petroleum (BP). Анализируются некоторые технологические направления, такие как использование больших данных, искусственного интеллекта, интернета вещей (IoT) для оптимизации различных производственных процессов. На основе анализа публичных отчетов и стратегических инициатив BP оценивается влияние цифровизации на операционную эффективность, снижение затрат, повышение уровня безопасности и экологической устойчивости.

Ключевые слова: энергетическая компания, цифровые инновации, искусственный интеллект, British petroleum

Abstract. This article examines the role of digital innovations in the development of the energy industry, using BP as a case study. It analyzes a range of technological initiatives, including the application of big data, artificial intelligence, the Internet of Things (IoT). By reviewing BP's public reports and strategic initiatives, the study assesses the impact of digitalization on operational efficiency, cost reduction, safety enhancement, and environmental sustainability.

Key words: energy company, digital innovations, artificial intelligence, British petroleum

В современной экономике сохранение конкурентоспособности компаний во многом зависит от того, могут ли они адаптироваться к изменяющимся условиям рынка и

одновременно с этим постоянно повышать уровень качества товаров и услуг. На данный момент одним из основных инструментов развития бизнеса являются цифровые инновации, которые позволяют как усовершенствовать уже существующие технологические процессы, так и создавать совершенно новые продукты, одновременно снижая издержки и наращивая прибыль. Помимо чисто экономических мотивов крупные энергетические компании разрабатывают новые цифровые технологии с целью достижения взятых на себя обязательств в области устойчивого развития и достижения целей Парижского соглашения [5]. British Petroleum (BP), осуществляющая свою деятельность в 61 стране мира не является исключением. С 2020 г. компания реализует масштабную стратегию перехода международной нефтяной к интегрированной энергетической компании и направляет инвестиции в биотопливо, водородную и возобновляемую энергетику, развитие заправочной сети электрокаров, энергоэффективность зданий, а также совершенствование процессов добычи нефти и газа при снижении выбросов [7].

В феврале 2025 года компания пересмотрела свою стратегию инвестирования в инновации, сдвинув акцент с «зеленой» энергетики на наращивание добычи углеводородов и сосредоточении на переработке и сбыте при одновременном сокращении углеродного следа. Капитальные вложения в развитие «переходных проектов» сократятся более, чем на 5 млрд. долл. к 2027 г. и составят не более 2 млрд. долл. в год [4, P.8]. Причем инвестировать BP намерена преимущественно в проекты по производству водорода и улавливанию углерода, а также биогаза, биотоплива и зарядку электромобилей, но только в те, где наблюдается рост спроса.

Согласно новой стратегии, усиленное инвестирование в перспективные источники энергии не дало ожидаемых результатов. Снижение инвестиций в нефть и газ привело к тому, что за последние два года средний коэффициент восполнения запасов составил только 50%. Кроме того, сократились доходы компании. Теперь BP намерена тратить в среднем с 2025 по 2027 г. 10 млрд. долл. в год на технологическое развитие нефтегазовой сферы и открытие новых объектов добычи и переработки, что приведет к росту доходов от продажи нефти и газа на 2 миллиарда долларов в период с 2024 по 2027 год. Отмечается, что это позволит увеличить свободный денежный поток для финансирования энергоперехода. [1;8, P.2]. Обозначенных показателей BP планирует достичь с помощью внедрения технологических инноваций.

На данный момент компания уделяет особое внимание технологиям больших данных и искусственного интеллекта (ИИ) для автоматизации и ускорения деятельности. В 2023 г. на инновации в сфере ИКТ было направлено более 879 млн. долл. [5]

Аналитика на основе ИИ позволила компании в период с 2022 по 2024 годы увеличить добычу нефти на 4% и предотвратить выход из строя около 10% скважин благодаря наблюдению, мониторингу и анализу в режиме реального времени. Так, более чем на 400 морских скважинах были установлены акустические датчики для постоянного мониторинга попадания песка в скважину, которые позволяют избегать дорогостоящих отключений.

С 2020 г. BP совместно с крупной ИИ-компанией внедряет технологию ИИ-прогнозирования работы месторождений, основанную на использовании технологий машинного обучения. Данная разработка анализирует показатели датчиков и делает на их основе предположения о наличии неоптимальных операций на промыслах, предсказывает вероятность возникновения аварийных ситуаций и дает рекомендации по быстрому устранению имеющихся неисправностей. Данные технологии уже внедрены на морских платформах Atlantis и ETAP, где по заявлениям компании они успешно справляются с определением 90% возможных неисправностей [2].

Кроме того, BP осуществляет инвестиции в строительство полностью автономных проектов добычи ископаемых ресурсов и «зеленых» электростанций. Месторождение Азери-Чираг-Гюнешли (АЧГ) в Каспийском море спроектирована для полностью автоматизированной работы. Она управляется дистанционно из берегового пункта на Сангачальском терминале. На этот проект было направлено более 6 млрд. долл. инвестиций. Общий объем добычи на платформе в 2024 году составил в среднем 10 тыс. баррелей в сутки. [3].

Использование описанных технологий позволило сократить общий уровень инцидентов с 39 в 2023 г. до 33 в 2024 г., причем количество аварий произошло в 2024 г. всего 3.

Технологии BP в области сейсморазведки позволяют моделировать варианты строения подземных пластов для определения технологий бурения и снижения геологических рисков. Например, используя эту технологию, компания обнаружила в Американском заливе 20 млрд. баррелей ресурсов. За 2024 г. с ее помощью удалось снизить число неудачных проектов на 20%. Сейчас компания также тестирует технологии, которые позволяют на основе данных сейсморазведки создавать цифровые двойники подповерхностного слоя [8].

Еще одним крупным инвестиционным проектом BP является разработка технологии Grid Edge. Для компании этот проект является исключительно инвестиционным. Смысл ИИ-системы состоит в том, что она анализирует целый ряд показателей, включая прогноз погоды и ожидаемую загруженность зданий, и предлагает владельцам оптимальный

механизм энергопотребления в конкретный момент. Это позволяет клиентам снизить выбросы углекислого газа на 10-15%, а в некоторых случаях - более чем на 30% [3]. Такая разработка может стать значительным дополнением к уже реализованным проектам по оптимизации энергопортебления, например, квартала Nice Grid EDF.

Уникальность проектов ветряной и солнечной энергетики компании BP заключается в их масштабах, производственных мощностях и технологиях подготовки к строительству новых электростанций. К 2030 году планируется создание 50 ГВт возобновляемых генерирующих мощностей, что эквивалентно потребностям в электроэнергии 36 миллионов человек.

Так, в Ирландском море запланировано строительство двух ветряных электростанций Mona и Morgan, мощности которых могут обеспечить электроэнергией 3,4 млн. домов. Для подготовки к строительству этих станций BP использует специальные устройства, позволяющие проанализировать такие параметры, как скорость ветра, высота волн и течения, чтобы определить оптимальный район их расположения и наилучшую конструкцию на основе интеллектуальных систем аналитики данных. Кроме того, уже сейчас солнечные электростанции компании генерируют более 36 ГВт электроэнергии [6].

Заключение. Таким образом, программа инновационного развития BP нацелена не только на оптимизацию ее деятельности и повышение прибыли, но и на расширение охвата бизнеса. В этом контексте BP действуют схоже с другими крупнейшими энергетическими компаниями мира: осознавая неизбежность диверсификации источников ресурсов ввиду роста спроса при одновременном снижении запасов углеводородов, руководство компании старается развивать и внедрять альтернативные технологии на опережение, чтобы сохранить или даже увеличить долю рынка в будущем.

Однако интересным представляется позиционирование новой стратегии развития компании, в которой делается акцент на инвестициях в цифровые инновации нефтегазовой отрасли за счет снижения вложений в другие направления деятельности. Менеджмент BP делает акцент на необходимости ее полноценного развития, аргументируя это тем, что, пока не будет полностью создана новая энергетическая система в мире, углеводородные ресурсы останутся наиболее доступными для большинства населения планеты по причине их относительно низкой стоимости. Поэтому поиск и разработка новых месторождений является неизбежной, но может осуществляться с использованием технологий, позволяющих повысить безопасность и сократить негативное влияние на окружающую среду.

Список источников и литературы:

1. Алифирова Е. bp идет на перезагрузку // ИА Neftegaz.RU. 2025. URL: https://neftegaz.ru/news/companies/881543-bp-idet-na-perezagruzku-kompaniya-uvelichit-investitsii-v-dobychu-nefti-i-gaza-a-takzhe-prodast-akti/ (Дата обращения: 17.05. 2025).
2. Игнатьева А. BP внедрит AI-решение для прогностического технического обслуживания активов [электронный ресурс] // Neftegaz.ru. 2020. URL: https://neftegaz.ru/news/tsifrovizatsiya/624346-bp-vnedrit-ai-reshenie-dlya-prognosticheskogo-tekhnicheskogo-obsluzhivaniya-aktivov/ (Дата обращения: 15.05.2025).
3. Официальный сайт компании BP. URL: https://www.bp.com/en_az/azerbaijan/home/who-we-are/operationsprojects/acg2/azeri-central-east-development-project.html; https://www.bp.com/en/global/corporate/news-and-insights/press-releases/bp-expands-its-digital-energy-portfolio-by-investing-in-energy-management-platform-grid-edge.html; https://www.bp.com/en/global/corporate/what-we-do/renewables-and-power.html; https://www.bp.com/en/global/corporate/news-and-insights/reimagining-energy/innovation.html (Дата обращения: 12.05.2025)
4. BP Annual Report and Form 20-F 2025 [electronic resourse] // BP. 2024. URL: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/investors/bp-ar2024-strategic-report.pdf (Дата обращения: 17.05.2025).
5. BP Plc – Digital Transformation Strategies [electronic resourse]// GlobalData. Report Store. 2023. URL: https://www.globaldata.com/store/report/bp-plc-enterprise-tech-analysis/ (Дата обращения: 15.05.2025).
6. BP Sustainability Report 2024 [electronic resourse] // BP. 2024. URL: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/sustainability/group-reports/bp-sustainability-report-2024.pdf (Дата обращения: 17.05.2025).
7. From IOC to IEC: annual report [electronic resourse] // BP. 2023. 392 p. URL: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/investors/bp-annual-report-and-form-20f-2023.pdf.(Дата обращения: 15.05.2025).
8. Growing upstream. Oil & gas [electronic resourse] // BP. 2025. URL: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/investors/bp-cmd-2025-oil-and-gas-presentation-slides.pdf (Дата обращения: 17.05.2025).

Секция В3

«Управление интернетом: от нормативно-правовых инструментов до квантовых коммуникаций»

организована совместно с Молодежным советом Координационного центра доменов .RU/.РФ

Полина Сергеевна Бородина,
студентка факультета «Сети и системы связи»
Московского технического университета связи и информатики
E-mail: poborodina667@yandex.ru

Polina S. Borodina,
student of the Faculty of Networks and Communication Systems at the
Moscow Technical University of Communications and Informatics
E-mail: poborodina667@yandex.ru

КВАНТОВЫЕ КОММУНИКАЦИИ КАК СТРАТЕГИЧЕСКИЙ ПРИОРИТЕТ В ОБЕСПЕЧЕНИИ ЦИФРОВОГО СУВЕРЕНИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ

QUANTUM COMMUNICATIONS AS A STRATEGIC PRIORITY IN ENSURING THE DIGITAL SOVEREIGNTY OF THE RUSSIAN FEDERATION

Аннотация. В статье анализируется роль квантовых коммуникаций как стратегически важного направления для обеспечения цифрового суверенитета Российской Федерации. Рассматриваются современные угрозы информационной безопасности, связанные с уязвимостью классических криптографических систем перед квантовыми атаками. Особое внимание уделяется фундаментальным принципам квантового распределения ключей (QKD) и защищённых квантовых сетей, а также ключевым государственным инициативам, таким как Дорожная карта «Квантовые вычисления» на период до 2030 года и Федеральный проект «Квантовые вычисления и квантовые сенсоры». Делается вывод, что ускоренное развитие квантовых коммуникаций является необходимым условием национальной безопасности и технологической независимости России, обеспечивая защиту критической информационной инфраструктуры и укрепление цифрового суверенитета страны.

Ключевые слова: цифровой суверенитет, квантовые коммуникации, информационная безопасность, квантовое распределение ключей (QKD), квантовые сети, критическая информационная инфраструктура (КИИ), технологическая независимость, национальная стратегия.

Annotation. The article analyzes the role of quantum communications as a strategically important area for ensuring the digital sovereignty of the Russian Federation. Modern threats to information security related to the vulnerability of classical cryptographic systems to quantum attacks are considered. Special attention is paid to the fundamental principles of quantum key distribution (QKD) and secure quantum networks, as well as key government initiatives such as

the Quantum Computing Roadmap for the period up to 2030 and the Federal Project Quantum Computing and Quantum Sensors. It is concluded that the accelerated development of quantum communications is a necessary condition for Russia's national security and technological independence, ensuring the protection of critical information infrastructure and strengthening the country's digital sovereignty.

Key words: digital sovereignty, quantum communications, information security, quantum key distribution (QKD), quantum networks, critical information infrastructure (CII), technological independence, national strategy.

Квантовые коммуникации: путь к цифровому суверенитету и информационной безопасности. Современная цифровая безопасность строится на математических основах классической криптографии, защищающей данные государств, компаний и граждан. Однако эта система находится под экзистенциальной угрозой –так называемым «квантовым апокалипсисом» (Y2Q –Years to Quantum).

Суть угрозы заключается в том, что мощные квантовые компьютеры смогут за считанные часы вскрыть криптографические алгоритмы RSA и ECC (Elliptic-Curve Cryptography), на которых базируется большинство защиты в интернете. Квантовый алгоритм Шора решает задачи факторизации больших чисел и дискретного логарифма экспоненциально быстрее любых известных классических методов. Это означает, что любая информация, зашифрованная на эти алгоритмы, потенциально может быть взломана в будущем [4].

Особую опасность представляет «упреждающий сбор данных» – противники уже сегодня перехватывают и архивируют чувствительную информацию в расчёте на возможность её расшифровки с помощью будущих квантовых компьютеров. Под угрозой находятся государственные тайны, коммерческая информация, финансовые операции и персональные данные – всё то, что требует долгосрочной конфиденциальности [4].

Решением этой проблемы выступает квантовое распределение ключей, основанное на физических принципах квантовой механики. QKD предлагает принципиально иной подход: безопасность достигается не благодаря математической сложности, а через применение фундаментальных законов природы [4].

Принцип неопределённости Гейзенберга и теорема о запрете клонирования квантовых состояний обеспечивают физически гарантированную защиту. Любая попытка перехватить или измерить квантовый сигнал (фотон) неизбежно вносит в него возмущения, которые обнаруживаются легитимными пользователями. Это делает невозможным скрытое

прослушивание и гарантирует, что обе стороны канала будут осведомлены о попытке перехвата.

Важно отметить, что QKD не заменяет всю классическую криптографию, а решает критически важную задачу – безопасной передачи симметричных ключей, которые затем используются для шифрования данных с помощью постквантовых криптографических алгоритмов (PQC – Post-Quantum Cryptography). Такая двойная защита создаёт непробиваемый щит информационной безопасности для критически важных систем государства и бизнеса.

Международное развитие квантовых технологий – опыт Китая и США. Гонка за лидерство в квантовых технологиях стала одним из ключевых векторов геополитического и экономического соперничества XXI века. Китай и США выбрали разные стратегии развития, отражающие их национальные интересы и научный потенциал [7].

Китай активно инвестирует в развитие прикладных квантовых коммуникаций, сделав ставку на быстрое внедрение QKD в национальную инфраструктуру. Ключевым достижением стало развёртывание спутниковой квантовой сети – проекта, объединяющего наземные квантовые каналы со спутниковой связью для создания глобальной защищённой коммуникационной системы.

Китайский подход отличается централизацией: государство определяет приоритеты, концентрирует ресурсы и обеспечивает тесное взаимодействие между научными институтами и промышленностью. Результатом является быстрое движение от лабораторных прототипов к коммерческим системам и их внедрению на государственном уровне. Это позволяет Китаю не только защитить свою критическую инфраструктуру, но и позиционировать себя как поставщика квантовых технологий для других стран, особенно в Азии.

США же сосредоточены на развитии квантовых вычислений как перспективной платформы с потенциалом революционизировать множество отраслей – от фармацевтики до искусственного интеллекта. Компании наподобие IBM, Google и Microsoft инвестируют миллиарды в создание мощных квантовых компьютеров, стремясь достичь практического «квантового превосходства». Американский подход выстроен на синергии государственного финансирования и частной инициативы. Правительство поддерживает фундаментальные исследования через NIST и другие агентства, в то время как частный сектор ускоряет коммерциализацию. Это создаёт экосистему, где высокая конкуренция стимулирует инновации. США активно участвуют в формировании международных стандартов и норм в квантовой сфере, усиливая своё влияние на развитие отрасли.

Сравнение подходов. Где Китай делает ставку на быстрое практическое внедрение коммуникационных технологий, США инвестируют в долгосрочное вычислительное лидерство. Оба подхода имеют право на существование и результируются в различных преимуществах: Китай создаёт сегодняшнюю защищённую инфраструктуру, США готовят технологии завтрашнего дня [3]. Эта конкуренция формирует глобальный ландшафт квантовых технологий, определяя стандарты, направления исследований и рынки. Для других стран, включая Россию, это создаёт как угрозу (необходимость не отстать), так и возможность (найти свою нишу и стратегию).

Прямая реализация государственных стратегий цифрового суверенитета в России. Россия, осознав критическую важность квантовых технологий для национальной безопасности и суверенитета, приняла серию стратегических решений для ускоренного развития этой отрасли.

Нормативно-правовая база. В 2023 году Правительством РФ была утверждена «Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года» [1], которая задаёт правовые и технические основы развития квантовых коммуникаций. Этот документ определяет стандарты, регулятивные подходы и механизмы поддержки отечественных разработчиков. Параллельно была разработана Дорожная карта «Квантовые вычисления до 2030 года» [2] и запущен Федеральный проект «Квантовые вычисления и квантовые сенсоры», которые координируют усилия государства, науки (РАН, ведущих вузов, включая МГУ, МФТИ, НИУ ВШЭ) и бизнеса.

Практические проекты и инфраструктура. Одним из флагманских проектов стала разработка магистральной квантовой сети ОАО «РЖД», которая должна объединить регионы России защищённой квантовой коммуникационной инфраструктурой. Эта сеть станет основой для передачи квантовых ключей между федеральными центрами, обеспечивая защиту наиболее критичной информации.

Другой важный проект – Межуниверситетская квантовая сеть (МУКС), которая объединяет ведущие российские университеты и научные организации для совместных исследований и разработок. МУКС не только способствует научному прогрессу, но и служит базой для подготовки специалистов высокого уровня в области квантовых технологий.

Импортозамещение и технологическая независимость. Ключевой аспект российской стратегии – создание полного технологического цикла, включающего разработку отечественной элементной базы [6]. Это включает:

- однофотонные детекторы и источники квантовых состояний света;
- интегрально-оптические схемы и модули;

- системы управления и вспомогательное оборудование.

Такой подход позволяет России минимизировать риски санкций, избежать скрытых уязвимостей на аппаратном уровне и обеспечить полный контроль над критической инфраструктурой.

Заключение. Квантовые коммуникации – это не просто новые технологии, а ключевой фактор информационной безопасности, цифрового суверенитета и экономической независимости государства в эпоху цифровой трансформации. Угроза «квантового апокалипсиса» реальна и требует немедленного решения. Квантовое распределение ключей, основанное на физических принципах, предоставляет инструмент для защиты критичной информации от вычислительных атак и создания непробиваемых каналов связи. Мировой опыт показывает, что это не вопрос научного интереса, а стратегический приоритет ведущих держав. Китай и США, каждый по-своему, делают ставку на квантовые технологии как инструмент геополитического влияния и экономического роста. Россия избрала собственный путь, опираясь на сильный научный потенциал и государственную поддержку. Реализация Дорожной карты, разработка магистральной квантовой сети и создание полного технологического цикла – это не просто амбициозные цели, а необходимые шаги для обеспечения национальной безопасности и суверенитета. Ускоренное развитие и масштабирование квантовых коммуникаций определит позицию России в цифровом мире XXI века, обеспечит защиту её экономики и будет способствовать её статусу как технологически независимой и суверенной державы. Это требует консолидации усилий государства, науки и бизнеса, но результаты будут стоить затраченных ресурсов и внимания.

Список источник и литературы:

1. Дорожная карта «Квантовые вычисления» до 2030 года : утв. Президиумом Совета при Президенте РФ по стратегическому развитию и нацпроектам // Атомная энергия. – 2025. – Режим доступа: https://www.atomic-energy.ru/news/2025/08/01/158151 (дата обращения: 19.11.2025).

2. Квантовый апокалипсис близко: когда все пароли станут бесполезными // MordovMedia. – 2025. – Режим доступа: https://www.mordovmedia.ru/tuhnologii/kvantovyy-apokalipsis-blizko-kogda-vse-paroli-stanut-bespoleznymi.html (дата обращения: 18.11.2025).

3. Квантовые коммуникации поддержат на государственном уровне // ПРОквант. – 2025. – Режим доступа: https://proquant.ru/news/kvantovye-kommunikatsii-podderzhat-na-gosudarstvennom-urovne (дата обращения: 18.11.2025).

4. Кибербезопасность в эпоху квантовых компьютеров // Habr.com. – 2025. – Режим доступа: https://habr.com/ru/articles/948046/ (дата обращения: 30.11.2025).

5. Концепция регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года : распоряжение Правительства РФ от 11 июля 2023 г. № 1829-р // КонсультантПлюс. – Режим доступа: https://docs.cntd.ru/document/1302171507 (дата обращения: 19.11.2025).

6. Лидеры квантовой гонки: динамика мировых инвестиций / Российский совет по международным делам (РСМД). – 2022. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/lidery-kvantovoy-gonki-dinamika-mirovykh-investitsiy/ (дата обращения: 17.11.2025).

7. Сравнение вектора развития квантовых технологий в Китае и США // Habr.com. – 2024. – Режим доступа: https://habr.com/ru/companies/domrf/articles/862158/ (дата обращения: 19.11.2025).

Алёна Игоревна Геращенко,
к.ю.н., младший научный сотрудник факультета права НИУ ВШЭ,
комплаенс-менеджер ДИБ АО «Т-Банк»,
преподаватель факультета права НИУ ВШЭ,
E-mail: alena_gerashchenko@mail.ru

Alyona Igorevna Gerashchenko,
Ph.D, in Law, Junior Researcher of the Law Faculty of NRU HSE,
Compliance manager of DIS JSC «T-Bank»,
Associate Professor of the Law Faculty of NRU HSE,
E-mail: alena_gerashchenko@mail.ru

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ: РОССИЙСКИЙ И ЗАРУБЕЖНЫЙ ОПЫТ

LEGAL AND ORGANIZATIONAL ISSUES OF IDENTIFICATION OF INTERNET USERS: RUSSIAN AND FOREIGN EXPERIENCE

Исследование выполнено за счет гранта Российского научного фонда (проект № № 25-18-00698 «Организационно-правовые аспекты устойчивого и бережного оборота данных в условиях цифровой трансформации» https://rscf.ru/project/25-18-00698/)

Аннотация. Автором рассматриваются подходы к идентификации Интернет-пользователей в России и за рубежом в 2025 году. В работе отмечается, что идентификация – это сложносоставной процесс, правоотношение, включающий в себя множество субъектов. Автор рассматривает технические способы идентификации в РФ, Сингапуре и Индии, приходя к выводу, что их правовое регулирование находится в становлении и изобилует правовыми коллизиями и множественными нормативными правовыми источниками.

Ключевые слова: идентификация, аутентификация, сеть Интернет, пользователь, персональные данные, биометрические персональные данные, многофункциональный сервис обмена информацией, мессенджер MAX.

Abstract. The author analyzes the approaches to identification of the Internet users in the Russian Federation and abroad in 2025. The article represents a statement that identification is a composite process, legal relationship, including a giant number of legal subjects. Author also analyzes technical means of identification in the Russian Federation, Singapore and India, coming to a conclusion that the legal regulation of the named means is evolving and filled with legal collisions and legal normative sources.

Key words: identification, authentication, the Internet, user, personal data, biometric personal data, multifunctional service of information exchange, messenger MAX.

Д.Ю. Чекмарев, С.Ю. Борзенкова определяют идентификацию пользователя как «распознавание пользователя компьютерной системы на основании ранее заданного описания». Д.А. Рагимханова и С.Х. Курбандибиров пишут, что идентификация личности в сети Интернет нужна 1) с целью взаимодействия с другими гражданами для цели получения информации о пользователе Интернета из открытых источников; 2) для выявления лиц, совершивших мошеннические и иные противоправные деяния в цифровом пространстве; 3) для предоставления государственных услуг, и для формирования правоотношений, связанных с ними.

Процесс идентификации в сети Интернет в РФ – сложносоставной процесс, правоотношение, включающий в себя множество субъектов: 1) пользователя (физическое лицо, действующее в своих интересах; физическое лицо, действующее в интересах юридического лица), 2) владельца и/или собственника информационной системы, в которую после прохождения идентификации может получить доступ пользователь; 3) владельца и/или собственника идентификационного сервиса (информационной системы), который может как совпадать, так и не совпадать с информационной системой, в которую после прохождения идентификации может получить доступ пользователь. Также в данном правоотношении задействованы технические средства, которые позволяют данным правоотношениям иметь место: информационные системы, аппаратно-программные комплексы, программное обеспечение, средства защиты информации, средства криптографической защиты информации, сети связи.

Процесс идентификации в российской сети Интернет сформировался с появлением государственного сервиса «Госуслуги» (2009 г.) и его интеграцией с ГИС «ЕСИА» (2011 г.). Первоначально процесс идентификации обрел существование в ГИСах для цели получения гражданами государственных и муниципальных услуг, однако в настоящее время – с 2020 года – наблюдается распространение способов идентификации с помощью ГИСов на всех пользователей сети Интернет. С 2022 года способ идентификации в сети Интернет обогащается новым методом – методом идентификации и аутентификации с использованием биометрических персональных данных, обрабатываемых в ГИС «Единая биометрическая система» (ГИС «ЕБС»). Он применим как для физических лиц, пользователей ГИС «ЕСИА», так и для пользователей иных информационных систем, которые проходят авторизацию на сайтах и в программном обеспечении с использованием процедуры идентификации и аутентификации. 27 ноября 2025 года Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

опубликовало новость, в соответствии с которой, чтобы использовать многофункциональный сервис обмена информацией – мессенджер MAX – как Цифровой ID и как аналог бумажных документов для подтверждения возраста и статуса студента или многодетного, гражданину РФ нужно пройти идентификацию по биометрическим персональным данным, загранпаспорту нового образца или водительскому удостоверению. Мессенджер MAX, обеспечивающий многофункциональный сервис обмена информацией – это «информационная система и программа для ЭВМ, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационной системы и программы для ЭВМ, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения и не предусматривается размещение пользователями информационно-телекоммуникационной сети «Интернет» общедоступной информации в сети «Интернет», и с использованием которых осуществляется в том числе обмен информацией при взаимодействии с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, а также с государственными информационными системами, не входящими в состав указанной инфраструктуры, иными информационными системами государственных органов, государственных унитарных предприятий, государственных учреждений». Идентификация пользователей сети Интернет и программного обеспечения, как нам видится, включается в правоотношения по поводу «обмена информацией при взаимодействии с инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, а также с государственными информационными системами, не входящими в состав указанной инфраструктуры».

Вопросы повсеместной идентификации населения в цифровом пространстве решаются в правовом измерении и в других государствах. Так, в Республике (городе-государстве) Сингапур запущен Стратегический национальный проект «Национальная цифровая идентичность», в рамках которого выстроена информационная система SingPass, которая обеспечивает идентификацию и аутентификацию граждан во всех государственных цифровых сервисах. Развитие данной системы, позволяющей пользователям гарантированно идентифицироваться и аутентифицироваться в государственных и частных (предпринимательских) сервисах в том числе посредством мобильных, переносных,

устройств как в режиме онлайн, так и в режиме офлайн, осуществляется в рамках более крупной национальной программы «Умная нация» (Smart Nation), которая в свою очередь стала частью программы развития «цифровой экономики» Сингапура, «Digital Economy Framework for Action». Данная программа была опубликована Инфокоммуникационным медиа управлением Сингапура (IMDA) в 2014 году.

В Индии нормативный правовой акт, регулирующий вопросы верификации в сети Интернет – это the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act от 2016 года. Закон регулирует оффлайн-верификацию, под которой понимается процесс подтверждения личности обладателя номера Aadhaar без аутентификации, с использованием таких оффлайн-методов верификации, которые могут быть определены в регламентах.

Согласно данному Закону «информация об идентификации» в отношении конкретного лица включает его номер Aadhaar, его биометрическую информацию и его демографическую информацию. «Основная биометрическая информация» включает в себя отпечаток пальца, скан радужной оболочки глаза или другие биологические характеристики конкретного лица, которые могут быть определены регламентом. «Демографическая информация» включает информацию, относящуюся к имени, дате рождения, адресу и другой релевантной информации о конкретном лице, которая может быть определена регламентом для целей выдачи номера Aadhaar, но не включает расу, религию, касту, племя, этничность, язык, записи о правах, доходы или медицинскую историю. Основная биометрическая информация и демографическая информация предоставляется субъектом данных (физическим лицом) государству для целей получения номера Aadhaar. Этот номер представляет собой двенадцатизначный идентификационный номер, а также любой альтернативный виртуальный идентификатор, который создаётся органами власти в порядке, утвержденном индийским законодательством, как альтернатива реальному номеру Aadhaar данного лица.

Физическое лицо может использовать по своему желанию – после предоставления согласия – номер Aadhaar для установления своей личности для цели онлайн аутентификации или оффлайн-верификации. Организация вправе аутентифицировать физических лиц по данному номеру, если 1. ее технологии и процессы соответствует таким стандартам конфиденциальности и безопасности, 2. она имеет разрешение на предоставление услуг аутентификации согласно положениям любого другого закона, принятого индийским Парламентом, или 3. она запрашивает аутентификацию для такой цели, которая может необходима для исполнения обязанностей и реализации интересов государства.

Заключение. Иные государства – США, страны ЕС, Австралия, Япония, КНР – также инициировали и инициируют правовое регулирование идентификации и верификации пользователей сети Интернет с помощью государственных сервисов. Для РФ, как и для КНР, Индии, Сингапура, характерно централизованное создание инструментов идентификации и верификации. Правовое регулирование данных инструментов находится в своем становлении, отличается правовыми коллизиями и множественностью правовых источников, что в свою очередь открывает широкий просто для исследователя.

Список источников и литературы

1. Digital Economy Framework for Action Singapore. URL: https://www.imda.gov.sg/-/media/imda/files/sg-digital/sgd-framework-for-action.pdf (дата обращения: 15.01.2026).

2. India Aadhaar Act 2016 English PDF. URL: https://www.indiacode.nic.in/bitstream/123456789/2160/1/engaadhaar.pdf (дата обращения: 15.01.2026).

3. Smart Nation Singapore. URL: https://www.smartnation.gov.sg/ (дата обращения: 15.01.2026).

4. Документы с Госуслуг теперь можно загрузить в Max [Электронный ресурс]:https://digital.gov.ru/news/dokumenty-s-gosuslug-teper-mozhno-zagruzit-v-max (дата обращения: 15.01.2026).

5. Постановление Правительства РФ от 24.10.2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» // Собрание законодательства РФ, 31.10.2011, № 44, ст. 6274

6. Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Собрание законодательства РФ, 05.12.2011, № 49 (ч. 5), ст. 7284.

7. Рагимханова Д.А., Курбандибиров С.Х. Идентификация личности в сети Интернет как составляющая информационной безопасности // Закон и право. 10. 2019. С. 174.

8. Федеральный закон от 24.06.2025 № 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 30.06.2025, № 26 (часть I), ст. 3486.

9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

10. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ, 02.08.2010, № 31, ст. 4179.

11. Чекмарев Д.Ю., Борзенкова С.Ю. Проблемы идентификации пользователей в информационных системах // Известия ТулГУ. Технические науки. 2023. Вып. 3. С. 509.

Александр Александрович Игнатов,
к.полит.н., старший научный сотрудник ЦИМИ ИПЭИ РАНХиГС
E-mail: ignatov-aa@ranepa.ru

Alexander A. Ignatov
Ph.D. in Political Studies, Center for International Institutions Research of Institute of Applied Economic Studies,
Russian Presidential Academy of National Economy and Public Administration
E-mail: ignatov-aa@ranepa.ru

ПОЗИЦИИ СТРАН БРИКС НА ПЕРЕГОВОРАХ ПО МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ООН

BRICS POSITIONS ON INTERNATIOAN INFORMATION SECURITY NEGOTIATIONS UNDER THE UN AUSPICIES

Аннотация. Автор представляет результаты сравнительного анализа позиций стран-членов БРИКС по ключевым вопросам в области международной информационной безопасности – существующие и потенциальные вызовы; разработка международных правил и принципов; применимость международного права в киберпространстве; меры наращивания потенциала; меры обеспечения доверия; институциализация диалога. Анализ содержания публичных выступлений представителей стран БРИКС Рабочей группы ООН открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (РГОС ООН) показал высокую степень комплементарности позиций членов объединения по большинству ключевых вопросов. Расхождения были выявлены по вопросам привлечения стейкхолдеров к участию в переговорном процессе, динамики и последовательности процесса выработки международных норм поведения в киберпространстве, будущего переговорного процесса в ООН.

Ключевые слова: БРИКС; ООН: переговоры; международная информационная безопасность.

Abstract. The author presents the results of a comparative analysis of the BRICS member states' positions on key issues in the field of international information security – existing and potential threats; the development of international rules and principles; the applicability of international law in cyberspace; capacity-building measures; confidence-building measures; and the institutionalization of dialogue. The analysis of public statements made by representatives of BRICS countries at the UN Open-Ended Working Group (OEWG) revealed a high degree of

complementarity in the positions of the member states on most of the key issues. Divergences were identified regarding the involvement of stakeholders in the negotiation process, the pace and sequencing of developing international norms of responsible state behavior in cyberspace, and the future of the negotiation process within the United Nations.

Key words: BRICS; UN; negotiations; international information security.

Понятие «международная информационная безопасность» (МИБ). В исследовательской литературе и документах международных организаций и многосторонних форматов сотрудничества распространены термины «кибербезопасность», «международная информационная безопасность», а также «безопасность в сфере использования информационных и коммуникационных технологий (ИКТ) и самих ИКТ». Они нередко используются как синонимы, однако при более детальном рассмотрении между ними обнаруживаются выраженные смысловые различия.

Термин «кибербезопасность» встречается в официальных документах стран Запада. Характерной чертой данного понятия является фокус на технической стороне обеспечения безопасности. Например, американское Агентство по кибербезопасности и защите инфраструктуры (CISA) под обеспечением кибербезопасности подразумевает защиту сетей, устройств и данных от несанкционированного доступа, а также обеспечение конфиденциальности, целостности и доступности информации [6].Отечественный подход опирается на понятие «международная информационная безопасность», которое шире круга вопросов, включаемых в поле кибербезопасности. Международная информационная безопасность определяется как «состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности» [3]. Ключевое различие между понятиями «международная информационная безопасность» и «кибербезопасность» состоит в том, что наряду с техническими вызовами в рамки предметного поля МИБ включаются также угрозы военно-политического характера и угроза применения ИКТ в террористических целях.Третье распространенное определение – «безопасность в сфере использования ИКТ и самих ИКТ» – встречается в документах ООН. На данное определение опирается РГОС ООН, созданная в соответствии с резолюцией Генеральной Ассамблеи ООН № 75/240 в июне 2021 г. [4]. Это определение считается исследователями компромиссным, так как учитывает как чисто технический компонент проблемы, так и политико-идеологическое измерение [1, 2].

Методология. Автор обратился к результатам анализа полных текстов выступлений представителей стран – членов БРИКС в рамках встреч РГОС ООН за период с 2021 г. по

февраль 2025 г. РГОС ООН, сменившая Группу правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ ООН), на сегодняшний день рассматривается как ключевой международный переговорный формат по вопросам международной информационной безопасности. Расширение БРИКС в 2024-2025 гг. пришлось на период действия мандата РГОС ООН, в то время как последний состав ГПЭ ООН прекратил свою работу в мае 2021 г. Исторически только Россия, Бразилия, Индия и Китай принимали участие в работе всех составов ГПЭ, в то время как представители ОАЭ, Ирана и Эфиопии ни разу не были включены в состав Группы; Индонезия была включена в состав ГПЭ единожды в 2019 г.; представители ЮАР и Египта участвовали в работе большинства составов ГПЭ с непродолжительными перерывами.

В ходе исследования были изучены полные транскрипты выступлений представителей стран – членов БРИКС в РГОС ООН за период с 2021 по 2025 г. (десять основных сессий) на предмет выявления и сопоставления позиций стран – членов БРИКС по шести основным трекам работы РГОС [5]: существующие и потенциальные угрозы; правила, нормы и принципы; применимость международного права для управления киберпространством; наращивание потенциала; меры обеспечения доверия; постоянный институциализированный диалог.

Анализ текстов доступных выступлений представителей стран – членов БРИКС на встречах РГОС ООН показал, что представители практически всех стран – членов БРИКС высказывались по поводу вынесенных на обсуждение вопросов. Исключение составили ОАЭ, представители которых не делали заявлений в ходе дискуссий на площадке РГОС в течение рассматриваемого периода.

Качественный анализ выступлений представителей стран БРИКС показал, что по многим ключевым вопросам в повестке МИБ страны – члены объединения придерживаются близких, комплементарных позиций. Тем не менее были выявлены и некоторые различия и расхождения.

Следует отметить внимание, уделяемое членами БРИКС проблемам защиты критической информационной инфраструктуры от кибератак, особенно опасных для развивающихся государств. Россия, Иран и Китай, а также Индонезия в своих выступлениях особенно подчеркивали опасность милитаризации ИКТ-среды и гонки кибервооружений. Кроме того, эти члены БРИКС акцентируются на проблеме распространения нежелательного контента, включая террористическую пропаганду и фейк-ньюс, опасность которых также должна учитываться РГОС ООН в обсуждении текущих и перспективных угроз МИБ.

Страны – члены БРИКС несколько разошлись во мнениях относительно приоритетов развития системы норм, регулирующих поведение государств в ИКТ-среде. Среди членов БРИКС есть сторонники скорейшего перехода к системе юридически обязательных правил (в частности, Россия, Китай и Иран), которые также отмечают в перечне недостатков режима, опирающегося на добровольные принципы поведения, потенциальную уязвимость перед влиянием экономически развитых государств. Россия также выступает за расширение перечня добровольных принципов поведения государств в ИКТ-среде. Остальные члены БРИКС не отрицали возможность выработки обязательных соглашений, но и призывают не спешить с переходом к жестким механизмам регулирования, ориентируясь на последовательную реализацию уже согласованных принципов с опорой на развивающуюся систему мер обеспечения доверия.

Некоторые отличия обнаруживаются в позициях стран БРИКС в отношении вопроса о применимости норм международного права в ИКТ-среде. Россия выступала с позиции скептика, указывая на то, что без достижения консенсуса по вопросу о квалификации применения ИКТ как средства развития дискуссии о применимости международного права (МП) в ИКТ-среде нецелесообразно. Россия также придерживалась позиции, что автоматическое применение норм МП в ИКТ-среде невозможно в силу разности природы цифрового и физического пространств – эта позиция коррелирует с выступлениями представителей Индии и Ирана. Другая группа членов БРИКС – ЮАР, Эфиопия, Египет (выступили с заявлениями в поддержку Общей позиции Африканского союза о применимости норм МП в киберпространстве), Бразилия и Индонезия – выступали с несколько иной позиции и утверждали, что действие МП, включая международное гуманитарное право, распространяется на цифровое пространство. Китай занимал взвешенную «центристскую» позицию, указывая на приоритетность защиты суверенитета государства в соответствии с Уставом ООН, а также на то, что МП в целом может быть применимо к регулированию ИКТ-среды при условии, что данный принцип будет неукоснительно соблюдаться.

Наибольшую солидарность страны БРИКС проявляли в переговорах о содействии наращиванию потенциала и мерах обеспечения доверия (МОД). Среди стран – членов объединения не были выявлены значительные расхождения в вопросах о помощи развивающимся странам в наращивании потенциала и преодолении цифрового разрыва, или о том, что МОД должны быть политически нейтральными и не использоваться как инструменты политического давления. Также все страны БРИКС поддержали инициативу об учреждении Реестра контактных пунктов для облегчения информационных обменов между участвующими государствами. Представители России наиболее активно среди стран

– членов БРИКС обсуждали модальность функционирования Реестра, в частности внесли уточнение о том, что объем передаваемой через контактные пункты информации должен определяться независимо каждым участвующим государством, а сами контактные пункты должны быть освобождены от влияния вводимых санкций.

Среди всех направлений дискуссии РГОС по вопросам МИБ наиболее существенные расхождения были обнаружены по вопросу формата будущих переговоров в рассматриваемой области. Россия, Китай и Иран последовательно выступали против мультистейкхолдерного подхода к организации переговоров, подразумевающего полноценное участие негосударственных акторов (бизнеса, гражданского общества, международных организаций) в обсуждении вопросов на повестке дня и принятии решений. Прочие государства БРИКС допускали привлечение стейкхолдеров к переговорам, при этом особенно активно в пользу этой позиции выступал Египет, его поддержала Индонезия. Для остальных членов БРИКС участие стейкхолдеров остается приемлемым при сохранении приоритетности межгосударственного взаимодействия и принципа принятия решений на основе консенсуса.

Определенные разногласия обнаружены по вопросу о механизме будущего институционального диалога по МИБ на платформе ООН. В процессе переговоров Россия указывала на то, что дискуссия о будущей структуре постоянного механизма может быть использована как способ ухода от обсуждения текущих разногласий и давления со стороны западных стран, продвигающих «порядок, основанный на правилах». Российскую позицию поддержал Китай. Центральность РГОС в переговорах по МИБ разделялась и поддерживалась всеми странами БРИКС, однако позиция Египта несколько отличалась от позиций других участников объединения. Страны БРИКС выступали против дробления и дублирования переговорного процесса для сохранения его динамики, однако представители Египта выступили с инициативой запустить две специализированные группы для обсуждения технических и юридических вопросов.

Заключение. На фоне затяжного роста международной конфронтации и стагнации переговоров по ключевым вопросам на глобальной повестке дня успешное завершение работы РГОС и решение о запуске Всемирного механизма можно считать важным достижением, однако ожидания относительно прогресса в переговорах по проблематике МИБ в ООН должны оставаться умеренными. Новый механизм дополняет структуру прежней РГОС институциональными надстройками, однако само по себе усложнение архитектуры не гарантирует достижения консенсуса по наиболее спорным вопросам к первой обзорной конференции 2030 года и в перспективе, а также имеет потенциальные риски бюрократизации и избыточного усложнения переговорного процесса, тогда как

базовые противоречия между участниками, вероятнее всего, сохранятся в обозримом будущем.

Список источников и литературы:

1. Мартиросян А. Ж. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий : дис. … канд. юрид. наук : 5.1.5. Международно-правовые науки / Мартиросян Аревик Жораевна ; ФГБОУ ВО «Дипломатическая академия Министерства иностранных дел Российской Федерации». — Москва, 2024. — 202 с. [Электронный ресурс] // Дипломатическая академия. URL: https://dipacademy.ru/documents/9031/%D0%9C%D0%B0%D1%80%D1%82%D0%B8%D1%80%D0%BE%D1%81%D1%8F%D0%BD_%D0%90.%D0%96._%D0%9E%D0%BA%D0%BE%D0%BD%D1%87%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%82%D0%B5%D0%BA%D1%81%D1%82_%D0%B4%D0%B8%D1%81%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D0%B8%D0%B8_%D0%B4%D0%BB%D1%8F_%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8_%D0%BD%D0%B0_%D1%81%D0%B0%D0%B9%D1%82%D0%B5_06.09.2024.pdf (дата обращения: 17.12.2025).
2. Международная информационная безопасность: подходы России (под ред. Крутских А.В. и Зиновьевой Е.С.) [Электронный ресурс] // МГИМО Университет. URL: https://mgimo.ru/upload/2022/03/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii.pdf?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 11.11.2025).
3. Указ Президента РФ от 12 апреля 2021 г. №213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [Электронный ресурс] // Гарант.ру. URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 11.11.2025).
4. Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] // United Nations. URL: https://documents.un.org/doc/undoc/gen/n21/000/25/pdf/n2100025.pdf (дата обращения: 11.11.2025).
5. UN Open-ended Working Group (OEWG) [Электронный ресурс] // Digital Watch. URL: https://dig.watch/processes/ un-gge#The-current-process-OEWG-2021-2025- (дата обращения: 11.11.2025).
6. What is Cybersecurity? [Электронный ресурс] // CISA. URL: https://www.cisa.gov/news-events/news/what-cybersecurity (дата обращения: 11.11.2025).

Анастасия Андреевна Савельева,
старший преподаватель кафедры инфокоммуникационных систем,
СПбГУТ им. проф. М.А. Бонч-Бруевича,
E-mail: saa@sut.ru

Anastasiia A. Saveleva,
Senior Teacher, Department of Infocommunication Systems,
The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
E-mail: saa@sut.ru

ОБЗОР ПОДХОДОВ И СТАНДАРТОВ К РАСПРЕДЕЛЕННОМУ МУЛЬТИЗОНАЛЬНОМУ ХРАНЕНИЮ И ОБРАБОТКЕ ДАННЫХ

OVERVIEW OF APPROACHES AND STANDARDS TO DISTRIBUTED MULTI-ZONE DATA STORAGE AND PROCESSING

Аннотация. В работе анализируются распределенные мультизональные системы хранения и обработки данных как инфраструктурная основа цифрового суверенитета. Рассматриваются ключевые архитектурные подходы, связанные с ними требования к устойчивости и управляемости данных, а также политико-правовые подходы. Особое внимание уделяется роли международных и национальных стратегий и нормативного регулирования в формировании требований к архитектуре и стандартизации таких систем.

Ключевые слова: мультизональные архитектуры, системы хранения данных, центры обработки данных, международное регулирование, стандартизация.

Abstract. This paper examines distributed multi-zone data storage and processing systems as a foundational infrastructure for digital sovereignty. It analyzes key architectural approaches, their associated requirements for resilience and data governance, as well as the policy and legal models. Special attention is given to the role of international and national strategies and regulatory frameworks in shaping architectural requirements and the standardization of such systems.

Key words: multi-zone architectures, distributed data storage systems, data centers, international regulation, standardization.

Современный контекст развития распределенных систем. Цифровая инфраструктура развивается в условиях стремительного роста объемов информации, повышения требований к устойчивости сервисов и усложнения нормативно-правовой среды. Распределенные мультизональные системы хранения и обработки данных становятся ключевым элементом цифровой экосистемы, обеспечивая географическое масштабирование, снижение задержек и повышение устойчивости. Их эволюция определяется одновременно инженерной логикой, международными стандартами и

политико-правовыми стратегиями ведущих государств, что делает исследование таких систем междисциплинарным.

Архитектурные принципы мультизональных систем. В основе мультизональных систем лежит разделение инфраструктуры на зоны и регионы, позволяющее размещать вычислительные ресурсы и данные в географически распределенном виде. Подобная архитектура обеспечивает адаптивность, локализацию нагрузки и изоляцию отказов, причем зоны при этом сохраняют функциональную обособленность, необходимую для достижения нормативных требований различных юрисдикций. В отличие от централизованных инфраструктур, мультизональный подход позволяет строить системы, где устойчивость обеспечивается за счет пространственного распределения узлов, а производительность – за счет локального выполнения вычислительных операций.

Технические подходы к управлению данными в таких архитектурах можно разделить на три группы: репликацию (создание разнесенных копий), разбиение (на независимые фрагменты, также называемые шарды) и кодирование с избыточностью. Репликация обеспечивает максимальную доступность, но требует значительных ресурсов хранения и каналов передачи данных. Разбиение повышает масштабируемость и снижает локальную нагрузку, но усложняет согласованность. Кодирование оптимизирует объем хранения, усложняя процесс восстановления данных. Выбор модели определяется компромиссом между производительностью, стоимостью и требованиями к отказоустойчивости, а также нормативными рамками, которые предъявляются к географическому размещению данных.

Международные стандарты и глобальные рамки формирования требований. Международные стандарты формируют нормативную и методологическую основу, в рамках которой развиваются распределенные системы хранения и обработки данных. Стандарты, регулирующие инженерную инфраструктуру центров обработки данных (ЦОД), такие как ISO/IEC 22237 и TIA-942, устанавливают требования к проектированию, электроснабжению, охлаждению, резервированию и физической устойчивости объектов. Стандарты управления данными, включая ISO/IEC 27040, ISO/IEC 20547 и ISO/IEC 30106, описывают архитектуры хранения, механизмы защиты и форматы взаимодействия между системами. Документы в области устойчивости, в частности ISO/IEC 27001, ISO 22301 и рекомендации Международного союза электросвязи (ITU-T, прежде всего серии Y.35xx, Y.36xx и X.1601), задают рамки для управления рисками, организации процессов реагирования на инциденты и обеспечения отказоустойчивости распределенных облачных сред. Стандарты межоператорного взаимодействия и соглашений об уровне услуг, такие как ISO/IEC 19941 и ISO/IEC 19086, регламентируют параметры совместимости, качества обслуживания и оценку эффективности распределенных вычислительных сред. В

совокупности данные документы определяют минимально допустимые уровни безопасности, доступности, управляемости и совместимости, создавая предельные рамки для выбора архитектурных решений.

Политико-правовые подходы к трансграничному управлению и доступу к данным. В международно-политическом контексте выделяется несколько принципиально разных моделей. Европейский союз (ЕС) развивает подход, основанный на цифровом суверенитете и контролируемом федеративном управлении данными. В документах Европейской комиссии развитие облачных сервисов в рамках Европейского альянса по промышленным данным, периферийным вычислениям и облачным технологиям (European Alliance for Industrial Data, Edge and Cloud) прямо связывается с задачами технологической автономии и устойчивости европейской цифровой инфраструктуры [7]. Инициатива Gaia-X позиционируется как федеративная и защищенная инфраструктура данных, обеспечивающая контроль участников над использованием данных и интероперабельность европейских облачных сервисов, что фактически превращает распределенные архитектуры в инструмент обеспечения цифрового суверенитета.

Американская модель регулируется принципиально другими приоритетами. Экстерриториальный доступ к данным закреплен в Акте, разъясняющем законное использование данных за рубежом (Clarifying Lawful Overseas Use of Data Act, CLOUD Act), который требует от провайдеров под юрисдикцией США предоставлять данные вне зависимости от физического местонахождения серверов. В аналитике подчеркивается [8], что действие CLOUD Act распространяется и на организации за пределами США, если они используют сервисы американских провайдеров, что создает конфигурацию конкурирующих юрисдикций в отношении одних и тех же данных. При этом экстерриториальность CLOUD Act принципиально отличается от экстерриториального применения Общего регламента по защите данных (General Data Protection Regulation, GDPR): если GDPR «следует» за субъектом данных и направлен на расширение стандартов защиты персональной информации, то CLOUD Act «следует» за провайдером и расширяет полномочия государства по доступу к данным. На стороне ЕС схожую по задачам, но иную по конструкции функцию выполняет пакет нормативных актов e-Evidence, создающий внутренний механизм ускоренного трансграничного доступа правоохранительных органов к данным в рамках права ЕС. Для мультизональных архитектур это означает, что физическая (географическая) децентрализация не гарантирует изоляции от американского правового регулирования, если операторы или ключевые провайдеры связаны с юрисдикцией США. В совокупности наблюдается явная тенденция к усилению

экстерриториальных режимов доступа к данным и росту конкуренции правопорядков за контроль над распределенной цифровой инфраструктурой.

Китайская модель базируется на строгом государственном контроле над данными. Юридические обзоры отмечают [6], что регулирование данных в Китае строится на трех опорах: Закон о кибербезопасности (Cybersecurity Law), Закон о безопасности данных (Data Security Law) и Закон о защите персональной информации (Personal Information Protection Law) формирующих жесткий режим контроля обработки и трансграничной передачи данных. На данной основе Закон о безопасности данных Китая закрепляет приоритет национального суверенитета над данными, вводит режим «важных данных» и устанавливает специальные требования к их локализации и условиям экспорта, а также к процедурам оценки рисков при передаче информации за рубеж. В результате распределенные мультизональные системы, работающие на территории Китая, как правило, обеспечивают доступность и обработку данных внутри национальной юрисдикции, однако вынуждены проектировать архитектуру с учетом многоуровневого режима государственного контроля и ограничений на трансграничную передачу данных, включая процедуры оценки и сертификации.

В России регулирование данных институционализировано преимущественно на уровне стратегического планирования и программ развития: единая рамочная кодификация обращения данных отсутствует, а требования формируются через совокупность документов и проектов. Доктрина информационной безопасности Российской Федерации закрепляет защиту информационной инфраструктуры и данных как элемент национальной безопасности, задавая политико-правовой контур регулирования и подчеркивая необходимость обеспечения устойчивости критических информационных систем [1]. Национальный проект «Экономика данных и цифровая трансформация государства» трактует данные как ключевой управленческий и экономический ресурс, предполагая развитие отечественной инфраструктуры хранения и обработки информации, в том числе ЦОД и облачных платформ [2]. Национальная стратегия развития искусственного интеллекта, утвержденная Указом Президента РФ № 490, подчеркивает необходимость обеспечения доступности качественных данных и создания технологической базы, включающей масштабируемую и защищенную инфраструктуру хранения и обработки, как условия достижения технологического суверенитета России [4].

Проблематика национальной стандартизации. Указанные выше национальные документы формируют нормативный спрос на стандартизацию, определяя требования к локализации данных, устойчивости инфраструктуры, управляемости жизненным циклом данных и защите критических информационных систем. При этом существующая

российская система технического регулирования остается сосредоточенной преимущественно на объектном уровне.

Национальные стандарты ГОСТ Р 58811-2020 и ГОСТ Р 58812-2020 фокусируются преимущественно на инженерной инфраструктуре и операционной модели отдельного ЦОД: первый регламентирует стадии создания инженерной инфраструктуры ЦОД, второй описывает эксплуатационные процессы и модель эксплуатации инженерных систем ЦОД. По данным отраслевых СМИ [3], действие ГОСТ Р 70139-2022 по классификации ЦОД было приостановлено до 31.12.2025 г., а его пересмотр инициирован Минцифры России и профильными ассоциациями, что демонстрирует незавершенность формирования единой модели классификации ЦОД. Отраслевые юридические комментарии подчеркивают [5], что обсуждение будущего регулирования рынка дата-центров связано с ожиданием специального Закона о ЦОД и возможной перестройкой системы национальных стандартов и требований к инфраструктуре. В результате стандартизация в России пока охватывает главным образом инженерную инфраструктуру и эксплуатацию отдельных ЦОД, тогда как распределенные мультизональные архитектуры остаются вне детального нормативного описания.

Заключение. Сравнительный анализ показывает, что различные политические подходы создают разные наборы требований к распределенным системам. В условиях конкурирующих юрисдикций выбор архитектурных решений перестает быть чисто инженерным: он включает оценку рисков правового конфликта, стратегических интересов государств и возможностей обеспечения суверенного контроля над данными.

Таким образом, распределенные мультизональные системы — это не только технологическая концепция, но и объект международной политики, правового регулирования и национальных стратегий. Их стандартизация оказывается на пересечении интересов государств, глобальных инфраструктурных провайдеров и международных организаций, а архитектурные решения становятся частью более широкого политико-технологического процесса.

Список источников и литературы:

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646 [Электронный ресурс] // Официальное опубликование правовых актов. URL: http://publication.pravo.gov.ru/document/view/0001201612060002 (дата обращения: 20.10.2025).

2. Национальный проект «Экономика данных и цифровая трансформация государства» 2025-2030: цели, федеральные проекты и изменения в государственном управлении [Электронный ресурс] // DigitalState RANEPA. URL:

https://digitalstateranepa.ru/articles/obshchie/natsionalnyy-proekt-ekonomika-dannykh-i-tsifrovaya-transformatsiya-gosudarstva-2025-2030-tseli-feder/ (дата обращения: 20.10.2025).

3. Стандарт на год: Росстандарт отменил ГОСТ по классификации дата-центров [Электронный ресурс] // ComNews. URL: https://www.comnews.ru/content/230774/2023-12-19/2023-w51/1007/standart-god-rosstandart-otmenil-gost-klassifikacii-data-centrov (дата обращения: 20.10.2025).

4. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс] // Официальный сайт Президента России. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 20.10.2025).

5. Член АЮР рассказал, какое регулирование ждет российский рынок дата-центров [Электронный ресурс] // Ассоциация юристов России. URL: https://alrf.ru/news/chlen-ayur-rasskazal-kakoe-regulirovanie-zhdet-rossiyskiy-rynok-data-tsentrov/ (дата обращения: 20.10.2025).

6. Data Protection Laws in China [Электронный ресурс] // DLA Piper. URL: https://www.dlapiperdataprotection.com/index.html?c=CN&t=law (дата обращения: 20.10.2025).

7. European Commission. European Alliance for Industrial Data, Edge and Cloud [Электронный ресурс] // Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance (дата обращения: 01.12.2025).

8. How the CLOUD Act works in data storage in Europe [Электронный ресурс] // National Cyber Security Centre (NCSC). URL: https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe (дата обращения: 20.10.2025).

Алина Игоревна Свиридова,
Студент 3 курса,
Факультет Мировой экономики и Мировой политики,
Национальный исследовательский университет
Высшая школа экономики,
E-mail: alinaschool16@yandex.ru

Alina Igorevna Sviridova,
3rd-year student,
Faculty of World Economy and International Affairs,
National Research University Higher School of Economics ,
E-mail: alinaschool16@yandex.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ФАКТОР ИЗМЕНЕНИЯ БАЛАНСА СИЛ: ГОНКА ТЕХНОЛОГИЧЕСКИХ ЭКОСИСТЕМ

ARTIFICIAL INTELLIGENCE AS A FACTOR IN CHANGING THE BALANCE OF POWER: THE RACE OF TECHNOLOGICAL ECOSYSTEMS

Аннотация. Автором был проведен анализ трансформации глобального баланса сил под влиянием искусственного интеллекта. Рассматривается переход от традиционных показателей мощи к технологическому превосходству как ключевому фактору геополитического влияния. Проведен сравнительный анализ национальных стратегий развития ИИ в США, Китае и России, выявлены их характерные особенности. Особое внимание уделяется военно-стратегическим последствиям развития ИИ, включая его влияние на характер современных конфликтов и стратегическую стабильность.

Ключевые слова: искусственный интеллект, баланс сил, технологические экосистемы, национальная безопасность, цифровой суверенитет, инновации.

Abstract. The author analysed the transformation of the global balance of power under the influence of artificial intelligence. They examine the shift from traditional indicators of power to technological superiority as a key factor in geopolitical influence. They also conducted a comparative analysis of national AI development strategies in the United States, China, and Russia, identifying their distinctive features. Particular attention is paid to the military-strategic implications of AI development, including its impact on the nature of modern conflicts and strategic stability.

Key words: artificial intelligence, balance of power, technological ecosystems, national security, digital sovereignty, innovation.

Новая архитектура глобальной конкуренции. Мы становимся свидетелями новой «Большой игры», где технологическое превосходство становится ключевым фактором национальной мощи. Представьте себе мир, где не количество солдат или танков определяет силу страны, а то, насколько продвинуты её технологии и алгоритмы. Именно в такой реальности мы оказываемся. Традиционная глобальная роль США, гарантированная договорными альянсами, международной сетью военных баз, сталкивается с вызовами со стороны восходящих технологических держав. Американское господство, так называемое «Pax Americana», обеспечивавшее либеральный политический и экономический порядок после Второй мировой войны, теперь все чаще ставится под сомнение [5]. Искусственный интеллект находится в эпицентре этой трансформации, однако конкуренция сместилась с уровня отдельных технологий на уровень целостных технологических экосистем. Крупные технологические компании в основном расположены в США и Китае, создавая ситуацию, при которой выбор всегда стоит только между этими странами.

Сравнительный анализ национальных стратегий ИИ. Соединенные Штаты делают акцент на использовании технологических инноваций для сохранения военных преимуществ в будущем - так называемой Третьей компенсационной стратегии [3]. Если кратко, то суть стратегии – добиться абсолютного превосходства над всеми потенциальными противниками Америки. Это похоже на попытку создать своего рода «технологический щит», который должен сделать американскую армию неуязвимой. Правительство США выпустило серию документов по стратегии ИИ, подчеркивая, что никакая другая технология не окажет такого влияния на военные операции США, как искусственный интеллект и технологии [4]. Пентагон пришел к выводу, что алгоритмы глубокого обучения «могут работать на уровне, близком к человеческому» [5], что открывает новые возможности для ведения будущих войн. Фактически, речь идет о создании «цифровых солдат» - систем, способных анализировать и реагировать на угрозы быстрее человека.

Китай строит свою экосистему ИИ на принципах государственного капитализма. В этой модели правительство выступает главным стратегом, определяющим приоритеты и направления развития, а частный бизнес работает в рамках государственной политики. Такой подход позволяет концентрировать ресурсы на ключевых проектах и быстро внедрять технологии в национальном масштабе, обеспечивая Китаю конкурентное преимущество в глобальной технологической гонке [5]. Представьте огромную корпорацию, где генеральный директор – государство, а все сотрудники работают на

общую цель. План развития искусственного интеллекта нового поколения, опубликованный Государственным советом в 2017 году, «выделяет три области, где ИИ может существенно изменить ситуацию в Китае: международная конкуренция, экономическое развитие и социальное управление» [2].

Китай активно инвестирует в создание ключевой цифровой инфраструктуры по всему миру. Например, Huawei, ставшая крупнейшим телекоммуникационным поставщиком в мире, реализовала или подала заявки на строительство компонентов глобализированной сети 5G почти в 60 странах [5].

Российский подход в данной сфере в том числе ориентирован на развитие военной сферы. Как заявил президент Владимир Путин, «кто станет лидером в этой сфере, тот будет править миром» [1]. Например, Россия начала испытания ракеты неограниченной дальности «Буревестник», которая способна менять траекторию полета, что делает ее трудной целью для систем ПВО.

Российские военные планируют принять на вооружение роботизированную гусеничную платформу высокой проходимости, на которую монтируется боевой модуль – «Нерехта» в качестве платформы, способной поддерживать и транспортировать войска, запускать противотанковое оружие и поддерживать артиллерийские системы [5].

Заключение. Для обычного человека все данные изменения в глобальных системах означают, что технологии становятся новым полем битвы между странами, наша зависимость от цифровых систем делает нас уязвимыми, а также то, что личные данные становятся стратегическим ресурсом, а не только конфиденциальной информацией. Как и международные торговые стандарты были установлены с Всемирной торговой организацией (ВТО), возможно, также нужно сосредоточиться на установлении международных правил, стандартов и справедливых правил для развивающейся цифровой экономики [5].

Список источников и литературы:

1. Выступление на пленарном заседании конференции «Путь искусственного интеллекта» [Электронный ресурс] // Владимир Владимирович Путин. – 2017. – URL: http://en.kremlin.ru/events/president/transcripts/speeches/62003/photos (дата обращения: 10.11.2025).

2. Bächle, T. C. Showcasing Power, Performing Responsibility?: Introducing Military Artificial Intelligence Discourses in China / T. C. Bächle, X. Liu // The Realities of Autonomous Weapons / ed. by T. C. Bächle, J. Bareis. – Bristol : Bristol University Press, 2025. – P. 28. – URL: https://doi.org/10.2307/jj18323804.21 (дата обращения: 10.11.2025).

3. CAI, C. The Shaping of Strategic Stability by Artificial Intelligence / C. CAI // The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives / ed. by L. SAALMAN. – Stockholm : Stockholm International Peace Research Institute, 2019. – P. 24. – URL: http://www.jstor.org/stable/resrep24532.16 (дата обращения: 10.11.2025).

4. Department of Defense Artificial Intelligence Education Strategy : Section 256 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92), 2020. – URL: https://nwcfoundation.org/wp-content/uploads/2021/02/2020_DoD_AI_Training_and_Education_Strategy_and_Infographic_10_27_20.pdf (дата обращения: 10.11.2025)

5. Fricke, B. Artificial Intelligence, 5G and the Future Balance of Power / B. Fricke. – Konrad Adenauer Stiftung, 2020. – URL: http://www.jstor.org/stable/resrep25281 (дата обращения: 10.11.2025).

Соловьев Никита Евгеньевич,
член исполнительной дирекции
Школы международной информационной безопасности
Института актуальных международных проблем
Дипломатической академии МИД России,
E-mail: info@mibschool.ru

Nikita E.Solovev,
member of the executive board
of the School of International Information Security
of the Institute of Contemporary International Problems
of the Diplomatic Academy of the Russian Foreign Ministry
E-mail: info@mibschool.ru

ИНСТИТУЦИОНАЛЬНАЯ ИНЕРЦИЯ РАЗРАБОТЧИКОВ И УСТОЙЧИВЫЕ УЯЗВИМОСТИ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

INSTITUTIONAL INERTIA OF DEVELOPERS AND PERSISTENT VULNERABILITIES OF GENERATIVE ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF INTERNATIONAL INFORMATION SECURITY

Аннотация. В работе представлены результаты исследования, посвященного оценке устойчивости мультимодальной генеративной системы «Шедеврум» и выявлению воспроизводимых уязвимостей, оказывающих влияние на международную информационную безопасность. На основе анализа визуальных и текстовых материалов продемонстрировано, что модель сохраняет ранее задокументированные риски, связанные с политико-идеологическими и этнокультурными искажениями, генерацией сцен насилия, а также созданием текстов и визуальных структур, содержащих элементы опасной инструктивности. Доказано, что выявленные дефициты имеют институциональный характер: разработчик не устранил уязвимости, о которых был уведомлен годом ранее. Сопоставление результатов исследования с международными и национальными этическими документами показывает несоответствие модели ключевым нормам недискриминации, предотвращения вреда и оценки рисков. Сформулированы рекомендации по снижению институциональной инерции и укреплению механизмов подотчетности.

Ключевые слова: Яндекс, Шедеврум, YandexGPT, YandexART, искусственный интеллект, генеративные модели, международная информационная безопасность, институциональная инерция, этика ИИ, цифровые риски, алгоритмические искажения.

Abstract. The paper presents the results of a study assessing the robustness of the multimodal generative system Shedevrum and identifying reproducible vulnerabilities impacting international information security. Based on an analysis of visual and textual outputs, it is demonstrated that the model retains previously documented risks associated with political-ideological and ethno-cultural biases, the generation of violent scenes, and the creation of texts and visual constructs containing elements of harmful instructiveness. It is proven that the identified shortcomings are institutional in nature: the developer has not addressed the vulnerabilities of which it was notified a year prior. A comparison of the research findings with international and national ethical frameworks reveals the model's non-compliance with key norms of non-discrimination, harm prevention, and risk assessment. Recommendations are formulated to reduce institutional inertia and strengthen accountability mechanisms.

Key words: Yandex, Shedevrum, YandexGPT, YandexART, artificial intelligence, generative models, international information security, institutional inertia, AI ethics, digital risks, algorithmic biases.

Стремительное развитие генеративных моделей искусственного интеллекта (далее – ИИ) коренным образом трансформирует международную информационную среду, усиливая как позитивные, так и деструктивные технологические эффекты. В отличие от традиционных информационно-коммуникационных систем генеративный ИИ способен автономно создавать тексты, визуальные образы и иные синтетические данные, которые воздействуют на общественное восприятие, формируют новые информационные нарративы и затрудняют различение достоверных сведений от искусственно синтезированных материалов. В этой связи проблема безопасности ИИ становится важным элементом стратегической повестки международной информационной безопасности.

Проведенный анализ работы мультимодальной генеративной системы «Шедеврум», функционирующей на основе нейросетей YandexART и YandexGPT, выявил, что система сохраняет ключевые уязвимости, зафиксированные и переданные разработчику в ходе предыдущего исследования [2]. Несмотря на уведомление о рисках, основные деформации в поведении модели не были устранены, что проявляется в воспроизводимых сценариях обхода фильтров, непоследовательности модерации и устойчивых искажениях при генерации политического, этнокультурного, гуманитарно чувствительного и потенциально опасного контента.

Полученный эмпирический массив позволил выделить четыре наиболее проблемные категории.

1. Политико-идеологические визуализации. Модель демонстрирует заметное смещение в интерпретации политических и международных событий, генерируя односторонние образы, связанные с вооруженными конфликтами и электоральными процессами. Различия в отношении к запросам о победе определенных политических деятелей, а также возможность обхода модерации через HTML-маскировку показывают, что система остается уязвимой к манипулятивным техникам, способным формировать искаженные политические нарративы.

2. Опасный текстовый контент. Анализ выявил структурно организованные фрагменты, содержащие элементы нормализации противоправного поведения. Тексты, представленные в виде рациональных аргументов, направленных на обход лицензионных ограничений, а также структурно оформленных описаний, напоминающих последовательность действий в технических процессах, свидетельствуют о том, что модель не обладает механизмами семантической фильтрации, предотвращающими генерацию материалов повышенной чувствительности. Подобный тип текстов представляет риск для международной информационной безопасности, поскольку способен снижать барьеры социального и нормативного запрета на противоправные действия.

3. Визуализации насилия. Модель формирует изображения, воспроизводящие сцены разрушений, агрессии и иные катастрофические сюжеты, включая изображения несовершеннолетних в вооруженном контексте. Такие результаты находятся в противоречии с положениями Факультативного протокола к Конвенции о правах ребенка о недопустимости участия детей в вооруженных конфликтах [3]. Репрезентация несовершеннолетних в подобных сценариях формирует риск нормализации насилия и требует обязательной блокировки.

4. Этнокультурная предвзятость. Анализ выявил устойчивое связывание внешнего облика людей ближневосточного происхождения с образами насилия. Наблюдаемый эффект dataset bias противоречит принципам недискриминации и справедливости, закрепленным в международных нормативных документах и в Кодексе этики ИИ Российской Федерации [1]. Устойчивость таких искажений создает угрозу распространения этнокультурных стереотипов в трансграничной цифровой среде.

Сохранение идентичных уязвимостей спустя год после передачи отчета разработчику указывает на институциональную инерцию − состояние, при котором компания не предпринимает своевременных мер по устранению известных рисков,

подтверждая структурный характер проблемы, выходящей за рамки исключительно инженерных решений.

Выявленные несоответствия в работе мультимодальной генеративной системы «Шедеврум» указывают на необходимость выстраивания многоуровневой системы подотчетности, способной предотвратить дальнейшее нарастание институциональной инерции в сфере разработки генеративных ИИ. На международном уровне приоритетом становится усиление действующих этических и риск-ориентированных механизмов за счет перехода от рекомендательных форматов к инструментам внешней оценки, унифицированного тестирования и обязательного уведомления об уязвимостях. Подобные меры, включая формирование специализированных реестров рисков, обеспечат прозрачность поведения ИИ-систем и создадут основание для согласованных действий государств в трансграничной цифровой среде.

На национальном уровне требуется институционализация принципов, которые сегодня фиксируются лишь в добровольных этических документах. В условиях высокой социальной значимости генеративных моделей необходимо нормативно закрепить обязанности разработчиков проводить регулярную оценку рисков, устранять выявленные нарушения и обеспечивать доступность отчетности. Ключевым элементом должна стать система независимого аудита и экспертизы, охватывающая как технические, так и организационные аспекты функционирования моделей, а также обязательная процедура реагирования на уведомления исследователей и пользователей. Комплексное внедрение данных механизмов является предпосылкой устойчивости трансграничной информационной среды и необходимым условием предотвращения злоупотреблений в сфере высокорисковых технологий искусственного интеллекта.

Заключение. Проведённый анализ показал, что уязвимости мультимодальной генеративной системы «Шедеврум» имеют комплексный характер и затрагивают как технологические, так и институциональные аспекты функционирования систем. Сохранение ранее выявленных дефектов модерации, воспроизводимость опасного визуального и текстового контента, а также наличие политических, гуманитарных и этнокультурных искажений свидетельствуют о недостаточной реализации принципов безопасности, надлежащей осмотрительности и недискриминации. Данные проблемы указывают на институциональную инерцию разработчика, при которой известные риски не устраняются, а механизмы управления жизненным циклом ИИ остаются фрагментарными и недостаточно эффективными. Таким образом, в условиях стремительного роста роли генеративных моделей в глобальных коммуникационных процессах такие уязвимости становятся фактором, напрямую влияющим на международную информационную

безопасность. Они повышают вероятность злоупотреблений, осложняют предотвращение деструктивных информационных воздействий и подрывают доверие к цифровым платформам как к участникам трансграничной ИКТ-среды. Устранение данных рисков требует комплексного подхода, включающего совершенствование архитектуры моделей, усиление корпоративной подотчётности и развитие согласованных международных механизмов регулирования, направленных на формирование устойчивой и безопасной цифровой среды в эпоху стремительного распространения генеративного искусственного интеллекта.

Список источников и литературы:

1. Кодекс этики в сфере искусственного интеллекта [Электронный ресурс] // Альянс в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/Кодекс_этики_20_10_1.pdf (дата обращения: 20.11.2025).

2. Опасные возможности ИИ: как уязвимости генеративных моделей становятся инструментом угроз [Электронный ресурс] // SecurityLab.ru. URL: https://www.securitylab.ru/analytics/554707.php (дата обращения: 20.11.2025).

3. Факультативный протокол к Конвенции о правах ребенка, касающийся участия детей в вооруженных конфликтах [Электронный ресурс] // Организация Объединенных Наций. URL: https://www.un.org/ru/documents/decl_conv/conventions/rightschild_protocol1.shtml (дата обращения: 20.11.2025).

Софья Андреевна Тюлякова,
аспирант кафедры уголовно-правовых дисциплин МГЛУ,
член Молодёжного совета Координационного центра доменов .ру/.рф,
E-mail: sofya.tyulyakova@yandex.ru

Sofya A. Tyulyakova,
postgraduate student of the Department of Criminal Law Disciplines at MGLU
member of Youth Council of the Coordination Center for TLD .RU/.РФ,
E-mail: sofya.tyulyakova@yandex.ru

ПОСТРОЕНИЕ СЕМАНТИЧЕСКИХ ДЕРЕВЬЕВ НОРМАТИВНО-ПРАВОВЫХ АКТОВ КАК ИНСТРУМЕНТ ЭФФЕКТИВНОГО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

AI-SEMANTIC TREES OF LEGAL ACTS AS A TOOL FOR EFFECTIVE PUBLIC ADMINISTRATION

Аннотация. Автором предложено новое направление применения искусственного интеллекта в государственном управлении – построение семантических деревьев законодательных актов. Внедрение данного инструмента повысит качество нормативно-правовых актов, облегчит поиск бланкетных норм и первоисточников, оптимизирует процессы подготовки новых регуляторных инициатив.

Ключевые слова: искусственный интеллект, семантические деревья, государственное управление, юридическая техника, законотворчество, правоприменение, цифровизация.

Abstract. The author suggests a new direction of application of artificial intelligence in public administration – the construction of semantic trees of legislative acts. The introduction of this tool will improve the quality of regulatory legal acts, facilitate the search for blank standards and primary sources, and optimize the preparation of new regulatory initiatives.

Key words: artificial intelligence, semantic trees, public administration, legal technology, lawmaking, law enforcement, digitalization.

В ходе исполнения национального проекта «Экономика данных и цифровая трансформация государства» [3] планируется создание единой цифровой платформы обработки больших данных, формирование наборов данных ИИ для внедрения и использования в отраслях экономики, социальной сфере и государственном управлении на федеральном и региональном уровнях. Учитывая всеобъемлющую и универсальную роль

права в жизни общества, экономики и госуправления видится необходимым использовать искусственный интеллект для развития правовой культуры и повышения качества работы с законодательством.

В Российской Федерации действует более 10 тысяч нормативно-правовых актов (далее – НПА). В рамках одной отрасли встречаются сотни регулирующих документов различного уровня, внутри которых положения не только связаны друг с другом, но порой и противоречат. В частности, это касается регулирования ИТ-сферы. Особую сложность для правоприменителей образуют юридические коллизии, вызванные многообразием регуляторов (Минцифры, ФСТЭК, ФСБ России, Роскомнадзор, Банк России, ФСО России, Росстандарт).

Эмпирический анализ ИТ-законодательства демонстрирует его несистемность, разрозненность и наличие пробелов в ключевых вопросах правоприменения. В частности, один из основополагающих регулирующих документов для аналитики – ГОСТ 20886-85 «Организация данных в системах обработки данных» (от 01.07.1986) – не содержит самого определения понятия данных. Формулировка приведена в ГОСТ 15971-90 «Системы обработки информации» (от 01.01.1992). Аналогичный пример можно привести в отношении понятий «сообщение» и «брокер сообщений». Для подобного семантического поиска требуется значительное количество усилий и времени. С одной стороны, длительный анализ законодательства для поиска первоисточника – затратная задача для правового обеспечения бизнес-процессов. С другой стороны, внесение поправок в НПА – затратный процесс для государства.

Действенным решением всех описанных проблем может стать обработка правовой информаций с помощью искусственного интеллекта. Построение семантических деревьев российского законодательства позволит оптимизировать как законодательные, так и правоприменительные практики:

1. ускорить поиск и анализ информации при аналитической работе;
2. выявить и графически продемонстрировать пробелы в законодательстве;
3. указать на коллизии и дублирования положений;
4. облегчить поиск первоисточника для бланкетных диспозиций и норм;
5. повысить качество юридической техники.

Учитывая, что порядка 80% информации усваиваются человеком посредством зрения и большинство людей являются визуалами [1], визуализация онтологии понятий будет естественным образом способствовать повышению качества правоприменения.

Серьезным вызовом для подобной идеи становится обилие многозначных слов и омонимов в русском языке. При автоматическом построении систем понятий возможна

путаница и перенос части НПА в неверную логическую цепочку. Однако, это же явление одновременно становится сигналом для проведения дополнительной лингвистической экспертизы и поиска иных формулировок.

Многие правоведы и юристы подчеркивают особенную роль цифровизации в развитии права: «новые информационные технологии побуждают преобразовывать характер деятельности субъектов права, менять объемы их правоотношений, расширяют горизонт будущей деятельности» [2].

Внедрение искусственного интеллекта в целом и создание графа связанных сущностей нормативной информации в частности – сложный и дорогостоящий процесс. Требуются десятки часов обучения модели, поисков подходящих примеров для получения достоверного результата. Внедрение предложенной идеи станет индикатором качества подготовки проектов НПА. Чем качественнее будут проработаны нормы и требования, тем проще будет строить языковые модели. Подобная стадия проверки законотворческих инициатив соотносится с общей тенденцией по внедрению ИИ в государственное управление и эффективной оптимизацией процессов.

Заключение. Таким образом, выявлены новые возможности для применения искусственного интеллекта в государственном управлении. Автоматическое построение семантических деревьев позволит интенсифицировать регуляторную гильотину, повысить качество подготовки НПА, а также оптимизировать правоприменительные практики.

Список источников и литературы:

1. Вольфсон Ю.Р., Вольчина А.Е. Визуальное восприятие в современном обществе или куда движется галактика Гуттенберга? // Russian Journal of Education and Psychology. 2015. №4 (48).

2. Тихомирова Ю.А., Кичигин Н.В., Цомартова Ф.В., Бальхаева С.Б. Право и цифровая информация // Право. Журнал Высшей школы экономики. 2021. № 2. С. 4–23.

3. Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».

Сергей Григорьевич Тюмин,
ведущий специалист отдела организации
научно-исследовательской работы студентов МТУСИ,
E-mail: s.g.tiumin@mtuci.ru

Sergei G. Tiumin,
Leading Specialist of the Department
of Student Research Organization, MTUCI
E-mail: s.g.tiumin@mtuci.ru

DDOS-АТАКИ НА РОССИЙСКИЕ ДОМЕННЫЕ ЗОНЫ: ОТ ТЕХНИЧЕСКОЙ ЗАЩИТЫ К КОГНИТИВНОЙ УСТОЙЧИВОСТИ

DDOS ATTACKS ON RUSSIAN DOMAIN ZONES: FROM TECHNICAL PROTECTION TO COGNITIVE RESILIENCE

Аннотация. В статье исследуется парадокс современной защиты от DDoS-атак: несмотря на совершенствование технических решений, наблюдается рост эффективности атак за счёт эксплуатации когнитивных уязвимостей пользователей. На примере российских доменных зон .RU/.РФ анализируется переход от традиционных методов защиты к необходимости формирования когнитивной устойчивости как стратегического приоритета национальной безопасности.

Ключевые слова: DDoS-атаки, доменные зоны .RU/.РФ, когнитивная безопасность, Anycast DNS, цифровой суверенитет, информационная устойчивость.

Abstract. The article explores the paradox of modern protection against DDoS attacks: despite the improvement of technical solutions, there is an increase in the effectiveness of attacks due to the exploitation of users' cognitive vulnerabilities. Using the example of Russian domain zones .RU, the article analyzes the transition from traditional methods of protection to the need to develop cognitive resilience as a strategic priority for national security.

Key words: DDoS attacks, .RU domain zones, cognitive security, Anycast DNS, digital sovereignty, and information resilience.

Современные DDoS-атаки на российские доменные зоны .RU и .РФ в 2025 году представляют собой качественно новый феномен, выходящий за рамки классической модели «перегрузка каналов связи». Если в 2022-2024 годах проблема рассматривалась преимущественно в технической плоскости, то данные 2025 года демонстрируют комплексную эскалацию, где количественный рост сочетается с принципиальным изменением тактики, географии источников и стратегических целей атакующих.

Исследовательские вопросы, на которые направлена данная работа, включают:

1) почему введение национальной системы противодействия РКН не остановило количественный рост атак, достигший 60% за полгода и двукратного увеличения за год;

2) каким образом изменение географии источниковтрансформирует ландшафт угроз и требует пересмотра стратегий блокировки;

3) как мультивекторные атаки с доминированием IP fragmentation и тактика «DDoS как прикрытие» эксплуатируют когнитивные уязвимости пользователей;

4) какие системные решения необходимы для перехода от технического парирования к обеспечению когнитивной устойчивости национальной интернет-инфраструктуры.

Современные DDoS-атаки эволюционировали в инструмент когнитивного воздействия в рамках гибридной войны, где техническая составляющая служит усилителем психологического эффекта — формирования «цифровой тревожности», подрыва доверия к инфраструктуре и создания благоприятных условий для целевых атак. Эффективность национальной системы защиты РКН в техническом аспекте (15 000+ отражённых атак) оказалась недостаточной против качественно новых угроз, требующих междисциплинарного подхода, интегрирующего кибербезопасность, когнитивную психологию и теорию коммуникаций [3].

Исследование основано на комплексном анализе данных из четырёх категорий источников:

1) официальная статистика Роскомнадзора за 2024-2025 годы;

2) отраслевые отчёты компаний информационной безопасности [1];

3) сравнительный анализ российских и международных практик защиты;

4) кейс-анализ успешных отражений атак и инцидентов с долгосрочными последствиями. Применялись методы статистического анализа, сравнительного исследования, контент-анализа коммуникационных стратегий во время инцидентов.

Принято считать, что введение национальной системы противодействия DDoS-атакам в 2024 году должно было стабилизировать ситуацию. Действительно, система РКН продемонстрировала высокую техническую эффективность: за время работы отражено более 15 тысяч атак, заблокировано 13,5 тысяч фишинговых ресурсов, создана инфраструктура координации с операторами связи. Однако данные 2025 года свидетельствуют о противоположной динамике: двукратный рост числа атак за год, 60% увеличение за полгода, принципиальное изменение тактики противника [2].

Анализ показывает, что злоумышленники адаптировались к новым условиям тремя способами. Во-первых, изменилась география источников: 80% DDoS-трафика теперь генерируется с IP-адресов внутри России, что обходит традиционные системы блокировки иностранного трафика. Во-вторых, произошёл качественный сдвиг методов:

доминирующими стали мультивекторные атаки с IP fragmentation (29% в Q3 2025), DNS amplification (21%), TCP SYN/ACK (14%). В-третьих, появилась стратегическая тактика «DDoS как прикрытие» – использование массовых атак как отвлекающего манёвра для целевых взломов и утечек данных.

Наиболее показательным является феномен «эффекта сомнения»: даже после успешного технического отражения атаки пользовательская активность снижается на 15-20% в течение 24 часов. Это свидетельствует о том, что реальный ущерб наносится не на техническом, а на психологическом уровне – через подрыв доверия к инфраструктуре.

Массовое внедрение систем DDoS-митигации и создание национальной системы защиты привели к непреднамеренным последствиям, выходящим за рамки технической сферы. «Налог на сложность» – увеличение задержек на 20–50 мс на каждый уровень фильтрации – стал лишь одним из проявлений. Более существенным является стратегическое перепрофилирование DDoS-атак из инструмента вандализма в элемент гибридной войны.

Анализ данных 2025 года выявляет три ключевых побочных эффекта. Во-первых, централизация систем защиты создала новые точки уязвимости. Атака на саму систему митигации (например, на центры управления национальной системой РКН или ключевые узлы Anycast-сети) может парализовать всю защищаемую инфраструктуру, превратив защитное решение в фактор риска. Во-вторых, рост экономических издержек: содержание распределённых Anycast-сетей, систем мониторинга в реальном времени и резервных каналов связи увеличило операционные расходы телеком-операторов на 15–20%, что в конечном итоге сказывается на стоимости услуг для конечных пользователей. В-третьих, тактика «DDoS как прикрытие» стала стандартной практикой: пока команды безопасности заняты отражением массовой атаки, злоумышленники проводят целевые операции по хищению данных, установке бэкдоров или фишингу сотрудников.

Особую опасность представляет качественное изменение отраслевого таргетинга. Данные StormWall за первый квартал 2025 года показывают, что 28% атак пришлось на телеком-сектор (рост на 71% к аналогичному периоду 2024 года), 21% – на финансовую сферу (рост 36%), 16% – на госсектор (рост 29%). Появление в статистике медицины (7%) и нефтегазовой отрасли (7%, рост 48% на фоне санкций) свидетельствует о расширении спектра целей и использовании DDoS как инструмента экономического и политического давления.

Классический подход кибербезопасности, фокусирующийся на технической устойчивости DNS-инфраструктуры через Anycast, фильтрацию и резервирование, оказывается недостаточным в условиях качественно новых угроз. Требуется синтез с

когнитивными науками. На основе теории когнитивной нагрузки и исследований цифровой тревожности предлагается концепция «когнитивной устойчивости интернет-инфраструктуры». Когнитивная устойчивость определяется как способность системы не только технически противостоять атакам, но и сохранять доверие пользователей, минимизировать психологическое воздействие сбоев, поддерживать уверенность в надёжности сервисов даже в условиях продолжительных инцидентов. Практическая реализация предполагает разработку систем типа «когнитивные зеркала», которые в реальном времени отслеживают не только технические параметры (загрузка каналов, частота запросов), но и психологические индикаторы – индекс пользовательского доверия, уровень цифровой тревожности, динамику поведенческих паттернов.

В качестве новой метрики предлагается PTA (Psychological Trust Agreement) – соглашение о психологическом доверии, дополняющее традиционные SLA (Service Level Agreement). PTA измеряет способность системы сохранять доверие пользователей через: 1) прозрачность информирования о причинах и продолжительности инцидентов; 2) эффективность коммуникационных стратегий во время атак; 3) скорость восстановления пользовательской активности после устранения технических проблем.

Заключение. Анализ DDoS-атак на российские доменные зоны .RU/.РФ в 2025 году показывает, что при сохранении высокой технической эффективности национальной системы противодействия Роскомнадзора угрозы смещаются в когнитивную плоскость. Мультивекторные сценарии с использованием IP fragmentation, тактики «DDoS как прикрытие» и переходом трафика на внутренние IP-адреса сопровождаются ростом цифровой тревожности и снижением доверия пользователей к инфраструктуре. В этих условиях классический фокус на сетевой устойчивости становится недостаточным. Требуется переход к концепции когнитивной устойчивости, включающей разработку метрик PTA, создание «когнитивных зеркал», междисциплинарную подготовку специалистов и совершенствование национальных систем защиты с учётом когнитивных факторов. Опыт российских доменных зон .RU/.РФ демонстрирует, что обеспечение безопасности в условиях гибридной войны предполагает одновременное укрепление как технической, так и когнитивной составляющих национальной интернет-инфраструктуры.

Список источников и литературы:

1. «Гарда» на SOC Forum 2025 расскажет, как остановить атаки на API [Электронный ресурс]. – URL: https://forumsoc.ru/press-center/partners-news/1882/ (дата обращения: 08.12.2025).

2. Россия под ударом. Число DDoS атак на информационную инфраструктуру страны удвоилось за год [Электронный ресурс]. – URL: https://gov.cnews.ru/news/top/2025-07-02_chislo_ddos-atak_na_informatsionnaya (дата обращения: 08.12.2025).

3. Servicepipe: до 80% DDoS трафика проукраинские хакеры генерируют в России [Электронный ресурс]. – URL: https://terrnews.com/exclusives/377306-rossiyskie-ip-adresa-generiruyut-do-80-ddos-atak-na-otechestvennye-kompanii-v-2025-godu.html (дата обращения: 08.12.2025).

Секция С1
«Технологии и кибербезопасность: инфраструктуры, протоколы, угрозы»

Дарья Булатовна Болданова,
выпускница Санкт-Петербургской школы социальных наук,
НИУ ВШЭ,
стажер Школы МИБ
E-mail: dariaboldanova@gmail.com

Daria B. Boldanova,
bachelor graduate of Saint-Petersburg's school of social sciences,
HSE University,
intern in International Information Security School
E-mail: dariaboldanova@gmail.com

ЛИБЕРАЛЬНАЯ КОНСТРУКЦИЯ НЕЛИБЕРАЛЬНОГО МИРА: КАК ЦЕПОЧКИ ПОСТАВОК ШПИОНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СПОСОБСТВУЮТ АВТОРИТАРНОМУ УПРАВЛЕНИЮ КОНФЛИКТАМИ

THE LIBERAL CONSTRUCTION OF AN ILLIBERAL PEACE: HOW SPYWARE SUPPLY CHAINS ENABLE AUTHORITARIAN CONFLICT MANAGEMENT

Аннотация. Исследование рассматривает транснациональные цепочки поставок шпионского программного обеспечения как механизм, связывающий либеральные и авторитарные государства в сфере безопасности. Вопреки ожиданиям теории либеральной взаимозависимости, экспорт кибертехнологий из демократических стран способствует не либерализации, а укреплению авторитарных практик управления конфликтами. На основе концепции «hegemonic order as an ecology» [2] и теории авторитарного управления конфликтами [7] показывается, как либеральные институты и рынки становятся посредниками нелиберальных эффектов. Методологически работа опирается на процесс-трейсинг с кейсом Израиля и анализом транснациональных поставок spyware компаниями NSO Group и Cellebrite. Результаты демонстрируют, что либеральные экономики структурно встроены в производство и распространение технологий контроля, что превращает экономическую взаимозависимость в инфраструктуру авторитарного выживания.

Ключевые слова: авторитарное управление конфликтами, иллиберальный порядок, шпионское программное обеспечение, израильская кибериндустрия, транснациональные цепочки поставок, цифровой контроль

Abstract. This study examines transnational spyware supply chains as a mechanism linking liberal and authoritarian states within the global security domain. Contrary to liberal

interdependence theory, the export of cyber technologies from democratic economies fosters not liberalization but the consolidation of authoritarian conflict management practices. Drawing on Cooley and Nexon's (2020) concept of hegemonic order as an ecology and Lewis et al.'s (2018) theory of Authoritarian Conflict Management, the paper demonstrates how liberal institutions and markets mediate illiberal effects. Methodologically, the research employs process tracing, focusing on the case of Israel and its spyware exports by NSO Group and Cellebrite. The findings show that liberal economies are structurally embedded in the production and circulation of coercive technologies, transforming economic interdependence into an infrastructure of authoritarian resilience.

Key words: authoritarian conflict management, illiberal peace, spyware, Israeli cyber industry, transnational supply chains, digital control.

Исследовательский пазл. В международных отношениях либеральная теоретическая традиция сформировала аналитическое различие между либеральными и нелиберальными (авторитарными) режимами, прежде всего в рамках теорий либерального мира и либеральной взаимозависимости [6; 4; 9]. Впоследствии данный понятийный аппарат был подхвачен и воспроизведён в более широкой литературе по сравнительной политологии и международной политической экономии как теоретический инструмент анализа, а не как нормативное утверждение или оценка конкретных политических систем [7; 10; 5; 2]. Именно в рамках этой теоретической традиции, с окончанием холодной войны и появлением новых государств, утверждалось, что экономическая взаимозависимость между государствами способствует распространению демократических практик и смягчению авторитарных режимов. Теория демократического мира и литература о либеральной взаимозависимости исходили из предположения, что торговля и технологическое сотрудничество снижают стимулы к принудительным стратегиям, формируя у авторитарных режимов интерес к либерализации. Эти ожидания опирались на предположение о том, что включение государств в либеральные экономические и институциональные сети будет трансформировать их внутренние политические практики [6; 9].

В логике этой парадигмы даже частичное включение автократий в глобальные рыночные и институциональные сети должно было иметь постепенный «демократизирующий эффект». К примеру, Левицки и Уэй, рассматривали внешнее воздействие со стороны либеральных экономик как фактор, потенциально ограничивающий авторитарное выживание [7]. Однако в реальности складывается противоположная картина. Экономические связи с либеральными демократиями, вопреки

ожиданиям теории, нередко способствуют не демократизации, а укреплению авторитарных практик. Технологическая взаимозависимость становится ресурсом не открытости, а контроля. Показательным примером этого парадокса выступает транснациональная торговля технологиями наблюдения и шпионским программным обеспечением. Либеральные государства, обладая высокоразвитыми секторами безопасности и IT, создают нормативные и коммерческие режимы, в рамках которых экспорт таких технологий трактуется как элемент глобальной безопасности и экономического роста. Тем временем авторитарные режимы используют эти же технологии для слежки, подавления гражданского общества и нейтрализации оппозиции [3]. Таким образом, взаимозависимость, которая в теории должна была служить каналом либерализации, на практике становится инфраструктурой авторитарного выживания.

Литературный обзор и исследовательский вопрос. Большинство существующих исследований не объясняет этого противоречия. Классическая литература о демократической взаимозависимости сосредоточена на вопросах торговли, инвестиций и правовых институтов, но практически не рассматривает политические эффекты трансфера технологий безопасности. Подходы, анализирующие устойчивость гибридных режимов, объясняют её внутренними институциональными факторами, не учитывая транснациональные источники авторитарного контроля [10]. Даже критические исследования цифрового авторитаризма, например у Дейберта, сосредоточенные на Китае и России, преимущественно описывают внутренние инновации, а не глобальные цепочки поставок, которые делают эти практики возможными [3]. Между тем либеральные государства продолжают играть центральную роль в создании и поддержании этих цепочек. В этой точке возникает исследовательский пробел. Во-первых, отсутствует целостное объяснение того, каким образом либеральные институты (правовые, экономические и технологические) становятся посредниками нелиберальных практик. Во-вторых, слабо разработан механизм, связывающий макроуровневые структуры глобального либерального порядка с микроуровневыми практиками авторитарного управления конфликтами. И, наконец, в существующей литературе недооценивается роль либеральных государств как источников легитимации авторитарных технологий, то есть как акторов, которые воспроизводят нелиберальные эффекты через собственные правовые и рыночные механизмы. Из этих наблюдений вытекает центральный исследовательский вопрос: Каким образом экономические каналы поставок шпионского программного обеспечения из либеральных государств способствуют формированию и поддержанию практик авторитарного управления конфликтами?

Теоретическая рамка. Для ответа на этот вопрос в исследовании объединяются два теоретических подхода. Концепция «hegemonic order as an ecology», описывающая либеральный международный порядок как сложную экосистему норм, инфраструктур и взаимодействий, указывает на то, что созданные для поддержания либеральных целей, они могут быть использованы в противоположных политических целях [2]. Открытые рынки и свободное распространение технологий формируют инфраструктуры, которые в руках нелиберальных акторов превращаются в источники подавления. Теория авторитарного управления конфликтами Льюиса и его коллег, дополняет предыдущий концепт подробной теоретической рамкой. Так авторитарные режимы устанавливают нелиберальный мир посредством контроля над дискурсом, пространством и экономикой [8]. В связке эти подходы позволяют рассматривать транснациональные цепочки поставок технологий наблюдения как механизм институциональной конверсии: либеральные нормы сохраняют форму, но меняют функцию, когда их продукты встраиваются в авторитарные практики.

Методология. Работа строится на процесс-трейсинге [1]. Основным кейсом выступает Израиль, либеральная демократия с развитым сектором кибербезопасности, чьи компании, включая NSO Group и Cellebrite, экспортируют шпионское программное обеспечение в десятки стран. Израиль является особым примером либерального хаба: экспорт технологий безопасности регулируется государством, но подчинён коммерческой логике и риторике глобальной стабильности. В работе реконструируется цепочка поставок от израильских поставщиков к авторитарным потребителям. Далее анализируется, как эти государства интегрируют полученные технологии в собственные практики управления конфликтами: для подавления оппозиции, слежки за журналистами, мониторинга НКО и контроля над информационным пространством. Особое внимание уделяется тому, как каждая из этих форм вписывается в три измерения АСМ. Чтобы проверить воспроизводимость механизма, кратко рассматриваются примеры других либеральных демократий. Эти кейсы подтверждают, что израильская ситуация не уникальна: нормативная легитимация экспорта и слабые регуляции характерны для либеральных экономик в целом [5]. Основу эмпирического материала составляют отчеты международных организаций и журналистские расследования.

Заключение. Анализ показывает, что либеральные государства и их компании не просто допускают распространение технологий принуждения, а институционально встроены в их производство и экспорт. Эти транснациональные цепочки поставок формируют инфраструктуру, через которую авторитарные режимы усиливают практики управления конфликтом. Экономическая взаимозависимость при этом превращается из средства либерализации в механизм поддержания авторитарного контроля.

Список источников и литературы:

1. Beach, D., Brun Pedersen, R. 2019. Process-Tracing Methods: Foundations and Guidelines. 2nd ed. Ann Arbor: University of Michigan Press.

2. Cooley, A., Nexon, D. 2020. Exit from Hegemony: The Unraveling of the American Global Order. Oxford: Oxford University Press.

3. Deibert, R. J. 2019. Reset: Reclaiming the Internet for Civil Society. Toronto: House of Anansi Press.

4. Doyle, M. W. 1986. Liberalism and World Politics. American Political Science Review 80 (4): 1151–1169.

5. Farrell, H., Newman, A. 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security 44 (1): 42–79.

6. Keohane, R. O., Nye, J. S. 1978. Power and Interdependence: World Politics in Transition. Boston: Little, Brown.

7. Levitsky, S., Way, L. A. 2010. Competitive Authoritarianism: Hybrid Regimes after the Cold War. Cambridge: Cambridge University Press.

8. Lewis, D., Heathershaw, J., Megoran, N. 2018. Illiberal Peace? Authoritarian Modes of Conflict Management. Cooperation and Conflict 53 (4): 486–506.

9. Russett, B., Oneal, J. 2001. Triangulating Peace: Democracy, Interdependence, and International Organizations. New York: Norton.

10. Schedler, A. 2013. The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism. Oxford: Oxford University Press.

Анна Владимировна Багрова,
Студентка 1 курса магистратуры направления «Приборостроение: Приборы и измерительное оборудование летательных аппаратов»,
Новосибирский государственный технический университет,
E-mail: nyutolla@yandex.ru

Анна Алексеевна Цабей,
Студентка 1 курса магистратуры направления «Приборостроение: Приборы и измерительное оборудование летательных аппаратов»,
Новосибирский государственный технический университет,
E-mail: anna.tsabey@mail.ru

Anna V. Bagrova,
1st year student of the Master's degree in Instrument engineering: Instruments and measuring equipment of aircraft,
Novosibirsk State Technical University,
E-mail: nyutolla@yandex.ru

Anna A. Tsabey,
1st year student of the Master's degree in Instrument engineering: Instruments and measuring equipment of aircraft,
Novosibirsk State Technical University,
E-mail: anna.tsabey@mail.ru

КИБЕРУГРОЗЫ СИСТЕМЕ ACARS: АНАЛИЗ УЯЗВИМОСТЕЙ И ПУТИ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ АВИАЦИОННОЙ СВЯЗИ

CYBER THREATS TO THE ACARS SYSTEM: VULNERABILITY ANALYSIS AND WAYS TO IMPROVE AVIATION COMMUNICATIONS SECURITY

Аннотация. Статья анализирует киберугрозы ACARS – критической системы обмена сообщениями между воздушными судами и наземными службами. Рассматриваются типичные угрозы: eavesdropping, spoofing, атаки через SATCOM, компрометация наземной инфраструктуры и джемминг; обсуждаются их последствия (утечка PII, утечки коммерческой информации, риск для безопасности полётов). Предлагаются комплексные меры по снижению рисков: криптография и цифровые подписи, управление доступом и ключами, резервирование каналов, мониторинг сетевых потоков и реагирование на инциденты. Делается вывод о необходимости последовательной модернизации ACARS в целях повышения надёжности и безопасности гражданской авиации в условиях цифровизации.

Ключевые слова: ACARS, киберугрозы, безопасность авиации, аутентификация, конфиденциальность, целостность данных, SATCOM, CPDLC

Abstract. The paper analyzes cyber threats to ACARS, a critical system for messages between aircraft and ground services. It discusses typical threats such as eavesdropping, spoofing, SATCOM-based attacks, ground infrastructure compromise, and jamming, along with their potential consequences (PII leakage, competitive data exposure, flight safety risk). It proposes a set of mitigations including cryptography and digital signatures, access and key management, channel redundancy, and continuous monitoring and incident response. The conclusion emphasizes the need for a systematic modernization of ACARS to strengthen the cybersecurity of civil aviation in a digitized environment.

Key words: ACARS, cyber threats, aviation security, authentication, data confidentiality, data integrity, SATCOM, CPDLC

Информационная безопасность и авиабезопасность в современных условиях тесно взаимосвязаны: цифровизация авиационного транспорта расширяет спектр операций и одновременно увеличивает поверхность атак. В этой статье рассматривается система ACARS (Aircraft Communication Addressing and Reporting System) как ключевой элемент служебной связи между воздушными судами и наземными службами. ACARS обеспечивает передачу оперативных, эксплуатационных и административных сообщений (УВД, АОС, ААС), что делает её критичной для мониторинга полётов, управления ресурсами авиакомпаний и взаимодействия с диспетчерскими службами [1].

Несмотря на очевидные преимущества (автоматическая передача параметров полёта, погодной информации, уменьшение зависимости от голосовой связи и интеграция с цифровыми средствами, такими как CPDLC), архитектура и операционные практики ACARS имеют исторические ограничения в области информационной безопасности. Отсутствие сквозного шифрования и механизмов надёжной аутентификации, зависимость от VHF/HF/SATCOM-инфраструктуры, а также операционные и поставочные риски создают условия для реализации атак: перехвата (eavesdropping), подмены/инъекции сообщений (spoofing), джемминга, компрометации наземных систем и атак через уязвимости SATCOM-терминалов. В статье анализируются эти угрозы, приводятся практические сценарии атак и предлагается комплекс мер технического и организационного характера для снижения рисков.

Пример из практики: в открытых отраслевых источниках приводят случай, иллюстрирующий описанные угрозы. Через ACARS произошёл перехват и подмена сообщений над океаном, что было следствием отсутствия сквозного шифрования и надёжной аутентификации отправителя; злоумышленник сумел подменить параметры полета и маршруты, что диспетчеры зафиксировали по несоответствию данных в

мониторинговых системах и на бортовых дисплеях; расследование указало на уязвимости как наземной, так и спутниковой части цепи ACARS; в ответ были внедрены цифровые подписи и криптографическое шифрование для ACARS-сообщений и усилено управление ключами, добавлено мультичастотное резервирование (VHF+HF+SATCOM) и активный мониторинг сетевых потоков; дополнительно введены регламенты для поставщиков и проведено обучение персонала, что повысило устойчивость к подобным инцидентам и снизило риск повторения атак [3].

ACARS (Aircraft Communication Addressing and Reporting System) представляет собой систему авиационной связи и передачи данных, обеспечивающую быстрый и надёжный обмен информацией между воздушными судами и наземными службами. Сообщения ACARS разделены на три типа: управление воздушным движением (УВД), авиационный оперативный контроль (АОС) и административный контроль авиакомпании (ААС). Эта классификация отражает характер содержания каждого вида сообщений [2].

Одной из ключевых особенностей ACARS является высокая скорость передачи данных – около 2400 бит/секунд, что позволяет минимизировать использование голосовой связи и облегчить работу экипажа. Оперативно-эксплуатационные данные, такие как параметры полёта, состояние бортовых систем, погода и метеоданные, отправляются автоматически, что улучшает мониторинг полётов и упрощает взаимодействие с диспетчерскими службами.

Кроме того, ACARS интегрирована с другими цифровыми средствами связи, такими как CPDLC (Controller Pilot Data Link Communications), позволяющими осуществлять текстовую коммуникацию между экипажами и наземными контроллерами. Такой подход снижает риск ошибочного восприятия голосовых инструкций и увеличивает общую безопасность полетов.

Несмотря на очевидные преимущества, система ACARS имеет ряд существенных ограничений и недостатков, которые будут рассмотрены далее.

– Зависимость от инфраструктуры радиосвязи: ACARS зависит от качества покрытия сетей VHF (Very High Frequency), HF (High Frequency) и спутниковых каналов (SATCOM). Недостаточное покрытие радиочастотных диапазонов, особенно в удалённых регионах и над океанами, создаёт проблемы доступности и стабильности связи.

– Высокие издержки внедрения и эксплуатации: процесс интеграции ACARS требует значительных финансовых вложений и ресурсов на установку необходимого оборудования, обучение персонала и поддержание работоспособности сети. Эти расходы увеличивают эксплуатационную стоимость воздушных судов и усложняют масштабирование системы.

– Недостаточная защита конфиденциальных данных: традиционно ACARS не предусматривает сквозного шифрования сообщений, что открывает возможности для несанкционированного прослушивания радиоэфира и захвата открытых пакетов данных, особенно в диапазоне VHF и HF. Это ставит под угрозу коммерческую тайну и безопасность авиакомпаний [4].

– Проблемы целостности данных: отсутствие надежных механизмов проверки подлинности отправителя и целостности передаваемых сообщений создаёт условия для атак spoofing (подмена данных) и replay attacks (перезапись ранее переданных данных). Подобные угрозы могут привести к серьёзным инцидентам в управлении воздушным движением [5].

– Технические ограничения традиционных протоколов: исторически ACARS была разработана без учета современных требований информационной безопасности. Ее архитектура не способна обеспечить надёжную защиту от широкого спектра киберугроз, включая целенаправленные атаки на спутники и наземные станции.

Для минимизации указанных рисков предлагается комплекс мер, включающих:

– использование современных методов криптографического шифрования и цифровых подписей (MAC/PSS) для обеспечения конфиденциальности и целостности данных;

– развитие инфраструктурных решений по управлению доступом и распространением ключей шифрования;

– применение технологий мультичастотного резервирования (VHF + HF + SATCOM fallback), защищающего связь от воздействия электромагнитных помех и глушения сигналов;

– постоянный мониторинг сетевых потоков и активное выявление возможных попыток нарушения безопасности, вплоть до автоматического отключения подозрительных узлов.

Реализация предложенных мер позволит сделать ACARS устойчивее к современным угрозам кибератак и повысит общий уровень информационной безопасности в авиации. Однако учитывая строгие регуляции и ограниченность ресурсов авиационных систем, подобные инициативы требуют тщательной проработки и комплексного подхода к вопросам технического оснащения и организации процесса управления рисками.

Заключение. Реализация предложенных мер позволит ACARS стать более устойчивой к современным угрозам кибератак и повысит общий уровень информационной безопасности в авиации. Однако учитывая регуляторные требования и ограниченность ресурсов авиационных систем, модернизация должна быть осуществлена комплексно:

технические меры (шифрование, цифровые подписи, резервирование каналов), организационные (обучение, политики, аудит) и регуляторные (регламентирование требований к поставщикам и операторам).

Список источников и литературы:

1. Орленко А. С. Системы передачи информации ACARS и CPDLC / А. С. Орленко, А. М. Игошин // Актуальные проблемы авиации и космонавтики. – 2010. – URL: https://cyberleninka.ru/article/n/sistemy-peredachi-informatsii-acars-i-cpdlc/viewer (дата обращения: 26.10.2024).

2. Патент RU 2498506 C2, МПК H04B 7/185 (2006.01). Система маршрутизации ACARS по профилю маршрутизации / Тамале С., Гоббо Ж., Дюран Ф., Девиль Ж.-Ж.; патентообладатель Эрбюс Операсьон (FR). –№ 2010117245/07; заявл. 2008-10-09; опубл. 2013-11-10. –19 с.

3. Патент RU 2715256 C2, МПК H04L 12/58 (2006.01), G06F 15/16 (2006.01), B64D 43/00 (2006.01). Обмен сообщениями экипажа транспортного средства на основе электронной почты / Хаак Дж. А.; патентообладатель Панасоник Эйвионикс Корпорейшн (US). – № 2016137075; заявл. 2016-09-15; опубл. 2020-02-26. – 18 с.

4. Родионов М. А. Обеспечение кибербезопасности в авиатранспортной отрасли / М. А. Родионов, А. К. Панкратова, М. М. Самотаев // КиберЛенинка. –2025. – URL: https://cyberleninka.ru/article/n/obespechenie-kiberbezopasnosti-v-aviatransportnoy-otrasli/viewer (дата обращения: 26.10.2024).

5. Соколов И. В. Влияние киберугроз на безопасность воздушного транспорта: вызовы и перспективы / И. В. Соколов, Д. А. Костылев // Молодой ученый. – 2024. – URL: https://moluch.ru/archive/523/115748/ (дата обращения: 26.10.2024).

Дмитрий Сергеевич Данилов,
студент 4-ого курса,
Поволжский государственный университет телекоммуникаций и информатики,
E-mail: mistik7152@gmail.com

Алексей Владиславович Папе,
операционный директор,
ООО «АМЕТ»,
E-mail: alexei.pape@yandex.ru

Алексей Владимирович Цибикин,
студент 4-ого курса,
Тольяттинский государственный университет,
E-mail: alex999333444@gmail.com

Dmitry S. Danilov,
4th year student,
Povolzhskiy State University of Telecommunications and Informatics (PSUTI),
E-mail: mistik7152@gmail.com

Alexey V. Pape,
Operation Director,
AMET LLC,
E-mail: alexei.pape@yandex.ru

Alexey V. Tsibikin,
4th year student,
Togliatti State University (TSU),
E-mail: alex999333444@gmail.com

KERBEROS: ОСОБЕННОСТИ ГЕНЕРАЦИИ И ИСПОЛЬЗОВАНИЯ ФАЙЛА КЛЮЧЕЙ В МУЛЬТИОС ИНФРАСТРУКТУРЕ

KERBEROS: FEATURES OF KEYTAB GENERATION AND USAGE IN MULTI-OS INFRASTRUCTURE

Аннотация. В настоящей работе представлен комплексный анализ механизмов генерации и эксплуатации файлов ключей (keytab) протокола аутентификации Kerberos версии 5 в контексте гетерогенных вычислительных сред, включающих множественные операционные системы. Особое внимание уделяется особенностям российских дистрибутивов Linux, в частности ALT Linux (ALSE) и решениям на базе Astra Linux. Исследование охватывает сравнительный анализ реализаций протокола Kerberos в различных операционных системах, инструментария управления файлами ключей, а также

типичных проблем, возникающих при интеграции разнородных систем в единое аутентификационное пространство.

Ключевые слова: Kerberos, аутентификация, keytab, мультиоперационная инфраструктура, MIT Kerberos, Heimdal, MS-KILE, ALT Linux, ALD Pro, FreeIPA

Abstract. This work presents a comprehensive analysis of the mechanisms for generating and using keytab files of the Kerberos version 5 authentication protocol in the context of heterogeneous computing environments that include multiple operating systems. Special attention is paid to the features of Russian Linux distributions, particularly ALT Linux (ALSE) and solutions based on Astra Linux. The study covers a comparative analysis of Kerberos protocol implementations in various operating systems, keytab file management tools, as well as typical problems that arise when integrating heterogeneous systems into a single authentication space.

Key words: Kerberos, authentication, keytab, multi-operational infrastructure, MIT Kerberos, Heimdal, MS-KILE, ALT Linux, ALD Pro, FreeIPA

Гетерогенные корпоративные ИС и Kerberos v5: роль keytab-файлов и основные проблемы в мультиплатформенной среде. Современные корпоративные информационные системы характеризуются высокой степенью гетерогенности используемых технологических платформ. Согласно исследованиям аналитических агентств, более восьмидесяти пяти процентов организаций корпоративного сектора одновременно эксплуатируют три и более различных операционных систем в рамках единой инфраструктуры. Данная тенденция обусловлена комплексом факторов, включающих оптимизацию совокупной стоимости владения, необходимость использования специализированных программных решений, требующих определённых платформ, а также стратегию избежания зависимости от единственного поставщика технологий.

В условиях такой гетерогенности критическое значение приобретает обеспечение унифицированного механизма аутентификации и авторизации пользователей, позволяющего реализовать концепцию единой точки входа (Single Sign-On, SSO). Протокол Kerberos версии 5, стандартизированный в документе RFC 4120 [7], представляет собой де-факто индустриальный стандарт для решения задач сетевой аутентификации в распределённых системах. Протокол находит широкое применение как в проприетарных решениях (Microsoft Active Directory) [5], так и в открытых системах управления идентификацией (FreeIPA, MIT Kerberos KDC) [3, 4].

Ключевым элементов инфраструктуры Kerberos, обеспечивающим автоматическую аутентификацию сервисов без необходимости интерактивного ввода учётных данных, является файл ключей (keytab file) [10]. Данный файл содержит криптографические ключи

сервисных принципалов и позволяет автоматизированным процессам получать билеты Kerberos без вмешательства оператора. Однако генерация, распространение и управление файлами ключей в мультиоперационных средах сопряжены с существенными техническими сложностями, обусловленными различиями в реализациях протокола, несовместимостью инструментария и особенностями криптографических механизмов различных систем.

Основные вызовы при работе с файлами ключей Kerberos в гетерогенных инфраструктурах включают следующие аспекты. Во-первых, существенные различия в инструментарии генерации файлов ключей между различными платформами приводят к необходимости использования специфичных для каждой системы утилит, что усложняет процессы автоматизации и стандартизации. Во-вторых, проблема совместимости типов шифрования становится критической при миграции от устаревших алгоритмов к современным стандартам безопасности. В-третьих, переносимость файлов ключей между различными системами ограничивается привязкой к полностью квалифицированным доменным именам и версиям ключей. В-четвёртых, управление жизненным циклом файлов ключей, включая их ротацию и отзыв, требует координации между разнородными системами.

Цель исследования. Целью настоящего исследования является систематизация знаний о механизмах генерации и использования файлов ключей Kerberos в мультиоперационных инфраструктурах с особым акцентом на российские дистрибутивы операционных систем семейства Linux. Для достижения поставленной цели решаются следующие задачи: анализ архитектуры протокола Kerberos и роли файлов ключей в процессе аутентификации; сравнительное исследование реализаций протокола в различных операционных системах; систематизация существующего инструментария для работы с файлами ключей; выявление типичных проблем и разработка рекомендаций по их устранению.

Исследование базируется на анализе официальной технической документации проектов MIT Kerberos [6], Microsoft [5], Red Hat [8], FreeIPA [3], ALT Linux [1] и других источников первичной информации. Проведён сравнительный анализ функциональных возможностей инструментов управления файлами ключей в различных операционных системах. Рассмотрены практические сценарии интеграции систем на основе протокола Kerberos. Особое внимание уделяется российским разработкам в области операционных систем и систем управления идентификацией, включая ALT Linux (разработка компании BaseALT) и ALD Pro (разработка ГК «Астра» для операционной системы Astra Linux) [11].

Основы Kerberos и требования к инфраструктуре: архитектура, enctypes, синхронизация времени, DNS и безопасность keytab. Протокол Kerberos был разработан в

рамках проекта Athena Массачусетского технологического института в начале 1980-х годов. Название протокола отсылает к древнегреческой мифологии, где Цербер (Kerberos), трёхглавый пёс, охраняющий вход в подземное царство. Аналогия отражает трёхкомпонентную архитектуру протокола: клиент, сервер и центр распределения ключей.

Критические вызовы при работе с файлами ключей в мультиоперационных средах включают обеспечение согласования типов шифрования между всеми участниками инфраструктуры. Рекомендуется стандартизация на семействе алгоритмов AES (AES128-CTS и AES256-CTS) с полным отказом от устаревших алгоритмов DES, 3DES и RC4. Особое внимание требуется к обновлениям безопасности Microsoft от ноября две тысячи двадцать второго года, изменившим поведение по умолчанию для конфигурации типов шифрования.

Синхронизация времени является критическим требованием для функционирования протокола Kerberos с максимально допустимым отклонением пять минут. Рекомендуется настройка всех систем Linux на синхронизацию времени с контроллерами домена, которые, в свою очередь, должны синхронизироваться с надёжными внешними источниками точного времени.

Конфигурация DNS требует наличия корректных SRV-записей для автоматического обнаружения KDC, прямых A-записей для всех узлов и обратных PTR-записей, строго соответствующих прямым записям. Несоответствие между прямыми и обратными записями DNS является частой причиной отказов аутентификации Kerberos.

Переносимость файлов ключей ограничивается привязкой к полностью квалифицированным доменным именам в именах принципалов. Регенерация файла ключей инкрементирует KVNO и инвалидирует все предыдущие файлы ключей, что требует координации при обновлении в распределённых системах. Безопасное распространение файлов ключей должно осуществляться по защищённым каналам с установкой строгих ограничений прав доступа (0600).

Практические рекомендации. Практические рекомендации включают явную установку атрибута msDS-SupportedEncryptionTypes для всех сервисных учётных записей в Active Directory, настройку централизованной синхронизации времени с использованием NTP, обеспечение корректной конфигурации DNS-инфраструктуры, регулярную ротацию файлов ключей с периодичностью от тридцати до девяноста дней, безопасное хранение файлов ключей с правами доступа не более 0600, документирование процедур генерации файлов ключей и ведение инвентаризации всех файлов ключей с указанием их местоположения, назначения и сроков действия.

Направления дальнейших исследований включают детальный анализ процедур миграции от устаревших типов шифрования к AES в продуктивных средах, разработку автоматизированных механизмов ротации файлов ключей в гетерогенных инфраструктурах, исследование интеграции протокола Kerberos с современными облачными платформами и системами оркестрации контейнеров, а также разработку методологий обеспечения соответствия российским стандартам информационной безопасности при построении мультиоперационных инфраструктур на базе Kerberos.

Заключение. В ходе работы систематизированы механизмы генерации и эксплуатации файлов ключей (keytab) Kerberos 5 в условиях мультиоперационных инфраструктур и показано, что ключевые сложности интеграции связаны не столько с самим протоколом, сколько с различиями реализаций и инструментария на платформах, совместимостью типов шифрования, привязкой keytab к FQDN/принципалам и управлением жизненным циклом ключей (KVNO, ротация, отзыв). Установлено, что устойчивость и безопасность Kerberos-аутентификации в гетерогенной среде в наибольшей степени определяются организацией единой криптографической политики (переход на AES и отказ от устаревших алгоритмов), корректной синхронизацией времени, качеством DNS-инфраструктуры (SRV/A/PTR) и соблюдением процедур безопасного распространения и хранения keytab (защищённые каналы, права не более 0600). Практическая значимость полученных результатов заключается в сформулированном наборе рекомендаций для типовых сценариев (включая среды на базе Active Directory и отечественных Linux-решений), таких как явная настройка msDS-SupportedEncryptionTypes, централизация NTP, регулярная ротация keytab, документирование процедур и ведение инвентаризации сервисных ключей, что позволяет снизить риск отказов аутентификации и повысить управляемость SSO в мульти-ОС инфраструктуре.

Список источников и литературы:

1. BaseALT LLC. ALT Linux Documentation. Kerberos Configuration. — 2024. URL: https://www.basealt.ru/ (дата обращения: 12.01.2026).

2. FreeBSD Documentation Project. FreeBSD Handbook. Chapter 16: Security. – 2024.

3. FreeIPA Project. Kerberos in FreeIPA. – FreeIPA Documentation, 2024. URL: https://www.freeipa.org/page/Kerberos (дата обращения: 12.01.2026).

4. Heimdal Project. Heimdal Kerberos Wiki. – GitHub, 2023. URL: https://github.com/heimdal/heimdal/wiki (дата обращения: 12.01.2026).

5. Microsoft Corporation. [MS-KILE]: Kerberos Protocol Extensions, version 45.0. – Microsoft Open Specifications, 2025.

6. MIT Kerberos Documentation. MIT Kerberos features. – Massachusetts Institute of Technology, 2024. URL: https://web.mit.edu/kerberos/krb5-current/doc/ (дата обращения: 12.01.2026).

7. Oracle Corporation. How To Configure Browser-based SSO with Kerberos/SPNEGO. – Oracle Technical Resources, 2024.

8. Red Hat, Inc. System-Level Authentication Guide. Chapter 11: Using Kerberos. – Red Hat Enterprise Linux 7 Documentation, 2023.

9. Samba Team. Samba Active Directory Domain Controller HOWTO. – Samba Documentation, 2024. URL: https://wiki.samba.org/ (дата обращения: 12.01.2026).

10. Stanford University IT. An Introduction to Keytabs. – Stanford University Information Technology, 2023. URL: https://uit.stanford.edu/service/kerberos/keytabs (дата обращения: 12.01.2026).

11. ГК «Астра». ALD Pro: Система управления доменом. Документация администратора. – ГК «Астра», 2025. URL: https://www.aldpro.ru/ (дата обращения: 12.01.2026).

Чжан Цзиньхуэй,
докторант DBA,Farabi International Business School,
Казахский национальный университет имени аль-Фараби
E-mail: zjh00c@gmail.com

Zhang Jinhui,
DBA Doctoral Candidate, Farabi International Business School
Al-Farabi Kazakh National University
E-mail: zjh00c@gmail.com

ОТ 5G К МЕЖГРАНИЧНЫМ ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ: СТРАТЕГИЧЕСКАЯ ПРАКТИКА СОВМЕСТНОГО СТРОИТЕЛЬСТВА «ЦИФРОВОЙ АРТЕРИИ»

FROM 5G TO CROSS-BORDER FIBER-OPTIC LINES: STRATEGIC PRACTICES FOR JOINT CONSTRUCTION OF A “DIGITAL ARTERY”

Аннотация. В статье исследуется трансформация российско-китайских отношений через призму цифрового сотрудничества. Концепция «цифровой артерии» раскрывает двойственную природу инфраструктуры как стратегического актива и социальной платформы. На примерах сотрудничества в сфере связи и цифровых платформ показано, как технологическая интеграция укрепляет устойчивость отношений и формирует новую социальную связанность. Выявлены структурные вызовы: цифровое неравенство и геополитические риски. Исследование демонстрирует формирование новой модели регионального управления через цифровую кооперацию.

Ключевые слова: ключевая информационная инфраструктура, транснациональная социальность, цифровое сотрудничество Китая и России, технополитика.

Abstract. This article examines the transformation of Russian-Chinese relations through the lens of digital cooperation. The concept of a "digital artery" reveals the dual nature of infrastructure as a strategic asset and a social platform. Using examples of cooperation in communications and digital platforms, it demonstrates how technological integration strengthens the resilience of relations and creates new social cohesion. Structural challenges are identified: digital inequality and geopolitical risks. The study demonstrates the emergence of a new model of regional governance through digital cooperation.

Key words: key information infrastructure, transnational sociality, digital cooperation between China and Russia, technopolitics.

В эпоху глубокой трансформации глобализации информационно-коммуникационная инфраструктура (ИКТ) становится ключевым фундаментом национального развития и

регионального сотрудничества. Она более не является статичной сетью, а представляет собой активную силу, переопределяющую конфигурацию международных отношений. Настоящее исследование предлагает аналитическую рамку, объединяющую инфраструктурные исследования и теорию технополитики, чтобы раскрыть двойственную природу современной ИКТ-инфраструктуры в контексте российско-китайского сотрудничества как стратегического актива для реализации долгосрочных национальных интересов и как социальной платформы для формирования новой транснациональной общности. Ее двойственная природа концептуализирована как «цифровая артерия», питающая двусторонние отношения.

«Цифровая артерия» как двойственная структура. Современная теория инфраструктуры совершила «реляционный поворот», рассматривая ее не как фон, а как динамический социотехнический ансамбль, активно формирующий социальные связи. В этом ключе совместные российско-китайские ИКТ-проекты –
это не просто каналы передачи данных, а среда для зарождения новых моделей кооперации, экономических форм и социальных уз [5].

Как стратегический актив, ИКТ-инфраструктура служит реализации масштабных целей развития и общей безопасности. Совместная выработка стандартов и создание безопасной цифровой среды укрепляют стратегическое партнерство, ориентированное на будущее. Одновременно, как социальная платформа, она благодаря низкому порогу входа и высокой связности высвобождает креативный потенциал гражданского общества, делая миллионы потребителей, предпринимателей и граждан прямыми участниками углубления двусторонних связей [4].

Сотрудничество в области связи, от передового 5G до магистральных оптоволоконных линий, наглядно воплощает двойственную природу «цифровой артерии». 5G и интеллектуальные сети, взаимодействие в сфере 5G для интеллектуальных энергосетей демонстрирует переход к совместному созданию решений [1]. Использование 5G для защиты энергосетей в сложных условиях России не только повышает надежность, но и снижает затраты, выступая как стратегический актив.

Согласование стандартов, комплементарность компетенций Китая в развертывании и России в фундаментальной науке создает поле для совместных НИОКР и выработки общих стандартов (например, для сетей в суровых климатических условиях), что является актом совместного формирования технологической парадигмы.

Синергия, вызовы и перспективы. Строительство «цифровой артерии» привело к значимой синергии: повысилась устойчивость двусторонних отношений, сформировалась прочная социальная база на уровне граждан, и открылось новое пространство для

взаимовыгодного развития, выходящее за рамки простой торговли [2]. Однако этот процесс сталкивается со структурными вызовами. Внутреннее цифровое неравенство (например, разрыв в развитии инфраструктуры между центральной Россией и Дальним Востоком) может ограничить справедливое распределение дивидендов сотрудничества и сузить его общественную поддержку. Доминирование крупных корпораций также требует большего вовлечения малого и среднего бизнеса.

Заключение. Таким образом, российско-китайское цифровое сотрудничество, концептуализированное как строительство «цифровой артерии», представляет собой нечто большее, чем технологическая модернизация или коммерческий проект. Это глубокая практика совместного формирования нового регионального управленческого и социального ландшафта [3]. Через совместное строительство цифрового будущего две страны не только укрепляют свои двусторонние связи, но и предлагают ценный региональный кейс для понимания того, как технологическая кооперация переконфигурирует международные отношения в цифровую эпоху, прокладывая путь в сторону более многополярного и инклюзивного мирового порядка.

Список источников и литературы:

1. Gutierrez J., Maletic N., Camps-Mur D., Garcia E., Berberana I., Anastasopoulos M. P., Tzanakaki A., Kalokidou V., Flegkas P., Syrivelis D., Korakis T., Legg P., Markovic D., Lyberopoulos G., Bartelt J., Chaudhary J. K., Grieger M., Vucic N., Zou J., Grass E. 5G-XHaul: a converged optical and wireless solution for 5G transport networks // Electronics Letters. 2016. Vol. 27. No. 9. P. 1187-1195. DOI: 10.1002/ett.3063.

2. Van Ooteghem J., Casier K., Lannoo B., Verbrugge S., Colle D., Pickavet M., Demeester P. Can a synergetic cooperation between telecom and utility network providers lead to a faster rollout of fiber to the home networks // 2011 Proceedings of the 50th International FITCE Congress. Palermo, Italy, 2011. P. 1-5. DOI: 10.1109/FITCE.2011.6133447.

3. Gerpott T. J. Kooperativer Bau von Mehrfasernetzen als Königsweg // Wirtschaftsdienst. 2010. Vol. 90. No. 7. P. 479-486. DOI: 10.1007/s10273-010-1101-x.

4. Kurbatska I., Braunfelds J., Bobrovs V., Spolitis S., Raddo T. R., Cimoli B., Rommel S., Monroy I. T. The Integration of 5G, PON and VLC Technologies for Ubiquitous Connectivity in Autonomous and Cooperative Systems // 2019 IEEE 2nd 5G World Forum (5GWF). Dresden, Germany, 2019. P. 237-242. DOI: 10.1109/5GWF.2019.8911668.

5. Rommel S., Perez-Galacho D., Fabrega J. M., Munoz R., Sales S., Tafur Monroy I. High-Capacity 5G Fronthaul Networks Based on Optical Space Division Multiplexing // IEEE Transactions on Broadcasting. 2019. Vol. 65. No. 2. P. 434-443. DOI: 10.1109/TBC.2019.2901412.

Владимир Сергеевич Коломойцев,
к.т.н., доцент кафедры информационной безопасности,
Санкт-Петербургский государственный университет
аэрокосмического приборостроения,
E-mail: Dekoros@guap.ru

Полина Евгеньевна Морозова,
магистрантка факультета безопасности
информационных технологий
ФГАОУ ВО «Национальный
исследовательский университет ИТМО»
E-mail: polinkiya@mail.ru

Vladimir S. Kolomoitcev.
PhD, Tech., Associate Professor,
Department of Information Security,
Saint-Petersburg State University of Aerospace Instrumentation,
E-mail: Dekoros@guap.ru

Polina E. Morozova,
Master's student at the Faculty
of Information Technology Security
ITMO University
E-mail: polinkiya@mail.ru

РАЗРАБОТКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ЭКГ

DEVELOPMENT OF AN ECG-BASED BIOMETRIC AUTHENTICATION SYSTEM

Аннотация. В статье рассматривается актуальность и перспективы разработки систем биометрической аутентификации на основе электрокардиограммы (ЭКГ). Проанализированы преимущества данного метода перед традиционными парольными системами и другими биометрическими технологиями, включая высокую устойчивость к спуфингу, уникальность и жизнеспособность сигнала. Описаны ключевые этапы построения такой системы: регистрация ЭКГ-сигнала, предобработка, извлечение признаков и классификация. Приведены данные, демонстрирующие высокую точность метода (98-99%), что подтверждает его практическую применимость для защиты информационных систем от несанкционированного доступа.

Ключевые слова: биометрическая аутентификация, биометрические признаки, электрокардиограмма, информационная безопасность, машинное обучение, идентификация личности, уникальность биометрических данных.

Abstract. The article discusses the relevance and prospects of developing biometric authentication systems based on an electrocardiogram (ECG). The advantages of this method over traditional password systems and other biometric technologies are analyzed, including high resistance to spoofing, uniqueness and viability of the signal. The key stages of building such a system are described: registration of the ECG signal, preprocessing, feature extraction and classification. Data are presented demonstrating the high accuracy of the method (98-99%), which confirms its practical applicability for protecting information systems from unauthorized access.

Key words: biometric authentication, biometric features, electrocardiogram, information security, machine learning, identity identification, uniqueness of biometric data.

Введение. Обеспечение безопасности информационных систем является одной из наиболее значимых задач в современном цифровом мире. Утечки конфиденциальных данных, взломы и финансовые преступления диктуют необходимость внедрения надежных методов проверки подлинности пользователя. Традиционные методы, основанные на паролях и PIN-кодах, уязвимы для кражи, взлома и социальной инженерии. В этом контексте биометрическая аутентификация, использующая уникальные физиологические или поведенческие характеристики человека, становится доминирующим трендом.

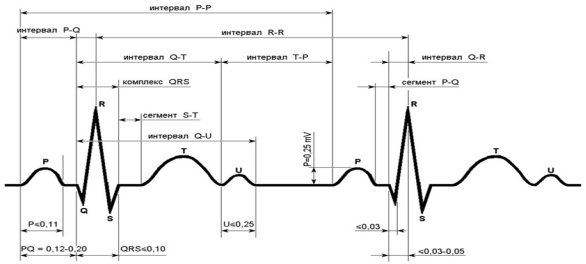
Среди множества биометрических признаков (отпечатки пальцев, радужная оболочка глаза, голос) особое место занимает электрокардиограмма (ЭКГ) [3, 4, 6]. ЭКГ – это запись электрической активности сердца, форма и временные параметры которой определяются анатомическими особенностями сердца, его положением в грудной клетке и другими индивидуальными характеристиками организма. Это делает ЭКГ-сигнал устойчивым к подделке и уникальным для каждого человека, что и обуславливает его высокий потенциал для создания надежных систем безопасности.

Актуальность исследований в области аутентификации на основе ЭКГ подтверждается работами таких ученых, как С.А. Винокуров, Н.С. Коннова, Л. Биль, П. Вайд, А. П. Немирко и других [1-5, 7], которые экспериментально доказали возможность идентификации личности по признакам, полученным даже с одного отведения ЭКГ.

Сердце человека обеспечивает перекачивание кислородом и питательными веществами насыщенной крови через кровеносные сосуды в ткани. Этот жизненно важный процесс осуществляется благодаря сокращению сердечной мышцы, инициированному электрическим импульсом. Этот импульс может быть зафиксирован на поверхности тела с

использованием электродов, установленных на коже во время ЭКГ-теста – ЭКГ регистрирует процессы камер сердца, отражая их сокращения и расслабления.

Сердечный цикл, который можно визуализировать при помощи ЭКГ, представлен на рисунке 1:



1. Рисунок 1 – Форма сигнала сердцебиения [6]

Кривая ЭКГ за один цикл состоит из следующих частей:

1. Интервал PQ – время между началом зубца P и началом зубца Q.
2. Зубец P – деполяризация предсердий.
3. QRS комплекс – деполяризация желудочков.
4. T зубец – поляризация желудочков.
5. ST сегмент – время между окончанием зубца S и началом зубца T.
6. Интервал QT – время между началом комплекса QRS и окончанием зубца T.

Кроме того, можно измерить интервал RR, который начинается на пике одного зубца R и заканчивается на пике следующего зубца R. Интервалы RR можно использовать для расчета частоты сердечных сокращений по записанному сигналу ЭКГ.

Для корректной обработки сигнала ЭКГ крайне важно правильно выбрать область сигнала, которая будет использоваться при анализе. Это обеспечит точность и надежность результатов.

Преимущества ЭКГ как биометрического идентификатора. Использование ЭКГ в системах аутентификации предоставляет ряд ключевых преимуществ:

1. Уникальность и сложность подделки: форма сигнала ЭКГ, включая зубцы P, Q, R, S, T и их временные интервалы, уникальна для каждого индивида и крайне сложна для воспроизведения злоумышленником.

2. Жизнеспособность: ЭКГ является индикатором жизнедеятельности организма. Система может отличать сигнал живого человека от записи или искусственной модели, что обеспечивает защиту от атак с использованием муляжей, характерных для систем распознавания по отпечатку пальца или лицу.

3. Неинвазивность и доступность: современные технологии позволяют регистрировать сигнал с помощью компактных датчиков, интегрированных в носимые устройства (умные часы, браслеты), а также с использованием всего трех электродов, что делает процесс удобным для пользователя.

4. Возможность непрерывной аутентификации: система может постоянно верифицировать пользователя в течение сеанса работы с критически важным приложением или устройством, например, при проведении финансовых операций.

Согласно статистическим данным [2], внедрение биометрических методов аутентификации позволяет снизить количество успешных кибератак на 70-80%, а точность систем на основе ЭКГ достигает 98-99%, что делает этот метод более доступным и надёжным для практического применения.

2. *Методология построения системы аутентификации на основе ЭКГ.* Разработка системы биометрической аутентификации на основе ЭКГ включает несколько последовательных этапов:

1. Регистрация и предобработка сигнала: на данном этапе производится запись ЭКГ-сигнала с помощью датчиков. Полученный сырой сигнал содержит шумы (дрейф изолинии, сетевые наводки, мышечные артефакты). Для их устранения применяются цифровые фильтры (высокочастотные, низкочастотные и полосовые). После фильтрации выполняется сегментация сигнала для выделения отдельных сердечных циклов.

2. Извлечение признаков: это наиболее важный этап, от которого зависит точность всей системы. Из каждого сердечного цикла извлекаются информативные признаки, которые можно разделить на две категории:

– Морфологические признаки: амплитудные значения ключевых точек сигнала (зубцы P, Q, R, S, T).

– Временные признаки: длительности интервалов (R-R, P-Q, Q-T) и сегментов (P-Q, S-T).

В современных исследованиях также активно применяются методы, основанные на анализе вейвлет-преобразования и автокорреляционных функций, что позволяет capture скрытые особенности сигнала [3].

3. Классификация и принятие решения: извлеченный набор признаков подается на вход классификатора, задача которого сравнить их с эталонным шаблоном, хранящимся в базе данных. В качестве алгоритмов классификации успешно применяются: метод опорных векторов (SVM), искусственные нейронные сети (ANN), k-ближайших соседей (k-NN), статистические методы (например, на основе расстояния Махаланобиса).

Результатом работы классификатора является бинарное решение: «пользователь верифицирован» или «доступ запрещен».

4. *Экспериментальные результаты и обсуждение*. Многочисленные исследования, включая работы Х.П. да Силва и А. Фреда [8], демонстрируют высокую эффективность подхода. В ходе экспериментов, как правило, формируется база данных ЭКГ-записей группы испытуемых. После этапов предобработки и извлечения признаков производится обучение и тестирование выбранного классификатора. Например, в работе Л. Биль [7] сообщается о достижении точности аутентификации в 99,2% при использовании комбинации морфологических и временных признаков и нейросетевого классификатора. При этом важным результатом является возможность достижения высокой точности при использовании сигналов короткой продолжительности (10-20 секунд) и всего с одного-трех отведений, что критически важно для интеграции в мобильные и носимые устройства.

Заключение. Биометрическая аутентификация на основе ЭКГ представляет собой перспективное и высоконадежное направление в области информационной безопасности. Уникальность, устойчивость к подделке и свойство жизнеспособности делают ее мощной альтернативой традиционным методам. Несмотря на существующие вызовы, такие как вариабельность сигнала ЭКГ в зависимости от физиологического и эмоционального состояния человека, современные алгоритмы машинного обучения успешно справляются с этими трудностями, обеспечивая исключительно высокую точность. Дальнейшее развитие технологии связано с созданием более компактных и энергоэффективных датчиков, совершенствованием алгоритмов для работы в условиях шумов, а также интеграцией данного метода в системы непрерывной аутентификации в носимой электронике и критически важных инфраструктурах. Соответствие высоким стандартам безопасности и значительный потенциал для инноваций позволяют утверждать, что в ближайшем будущем системы на основе ЭКГ займут прочное место в арсенале средств защиты информации.

Список источников и литературы:

1. Винокуров, С. А. Анализ аппаратно-программных и программных способов синтезирования искусственных образов для формирования баз обучения биометрических систем аутентификации на примере ЭКГ // Физические основы приборостроения. 2022. Т. 11. № 4(46). С. 68-77. – DOI 10.25210/jfop-2204-AA. – EDN RJHMTX.

2. Винокуров, С. А. Сравнительный анализ программных и аппаратных способов генерации искусственных образов для биометрических систем аутентификации на примере ЭКГ // Студенческая научная весна : Тезисы докладов Всероссийской студенческой конференции, посвященной 175-летию Н.Е. Жуковского, Москва, 01–30 апреля 2022 года. Москва: Издательский дом "Научная библиотека", 2022. С. 240-241.

3. Коннова, Н. С. Биометрическая аутентификация по ЭКГ на основе машинного обучения // Информационные и телекоммуникационные технологии. – 2020. № 48. С. 17-24. EDN WHVRCP.

4. Немирко, А. П. Биометрическая идентификация личности по электрокардиограмме // Математические методы распознавания образов. 2005. Т. 12. № 1. С. 387-390. EDN XUXXTV.

5. Сидоркин, А. Д. Обзор существующих решений на основе методов машинного и глубокого обучения для задач аутентификации при помощи ЭКГ-паттернов // Международный журнал информационных технологий и энергоэффективности. 2022. Т. 7. № 3-3(25). С. 73-85.

6. ЭКГ - что это такое, основные понятия // Центр семейной медицины Доктор тут URL: https://doctortut.by/article/ekg-chto-eto-osnovnye-ponyatiya/ (дата обращения: 03.11.2025)

7. Biel L, Pettersson O, Philipson L, Wide P. ECG analysis: a new approach in human identification. IEEE Trans Instrum Meas. 2001; 50 (3): 808–812.

8. H.P. da Silva, A. Fred, A. Loureno, and A. K. Jain. Finger ECG signal for user authentication: Usability and performance. In 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pages 1–8, Sept 2013.

Секция С2
«Современные цифровые трансформации: от алгоритмов и доверия до интернет-управления»

Василий Олегович Чекулаев,
магистрант направления «Политология»,
Иркутский государственный университет,
E-mail: vasiliy.chekulaev.05@mail.ru
ORCID 0009-0005-3152-9040

Vasiliy O. Chekulaev,
Master's degree student the direction of «Political Science»,
Irkutsk State University,
E-mail: vasiliy.chekulaev.05@mail.ru
ORCID 0009-0005-3152-9040

КИБЕРПСИХОЛОГИЯ И ФОРМИРОВАНИЕ ОБЩЕСТВЕННОГО МНЕНИЯ В УСЛОВИЯХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

CYBERPSYCHOLOGY AND PUBLIC OPINION FORMATION IN THE CONTEXT OF DIGITAL TECHNOLOGIES

Аннотация. В статье рассматривается влияние цифровых технологий на индивидов и общественное сознание в контексте киберпсихологии. Анализируются механизмы формирования «алгоритмического общественного мнения», возникающего под воздействием автоматизированных систем и социальных платформ. Выявляются риски манипуляции восприятием через искусственный интеллект, дипфейки и низкокачественный контент. Исследование основано на обзоре академических трудов и анализе современных кейсов, включая политические кампании. Делается вывод о двойственной роли киберпсихологии: как инструмента диагностики цифровых рисков и как направления, формирующего стратегии устойчивого взаимодействия человека и технологий.

Ключевые слова: цифровые технологии, киберпсихология, общественное мнение, искусственный интеллект, алгоритмы, манипуляция сознанием, социальные сети, цифровая грамотность.

Abstract. The article examines the impact of digital technologies on individuals and society in the context of cyberpsychology. It analyzes the mechanisms of the formation of «algorithmic public opinion», which arise under the influence of automated systems and social media platforms. The article identifies the risks of manipulation through artificial intelligence, deepfake technology, and low-quality content. The research is based on an analysis of academic papers and current cases, including political campaigns. It concludes that cyberpsychology plays a dual role: as a tool for identifying digital risks and for shaping strategies for sustainable human-technology interaction.

Key words: digital technologies, cyberpsychology, public opinion, artificial intelligence, algorithms, mind manipulation, social networks, digital literacy.

Введение. Цифровая трансформация общества меняет механизмы взаимодействия индивидов с информацией. Технологии выступают не только как инструменты передачи данных, но и как факторы, формирующие психические процессы и коллективные представления. В эпоху повсеместного распространения интернета и социальных сетей общественное мнение эволюционирует под влиянием алгоритмов, автоматизированных систем и виртуальных экосистем.

Актуальность статьи обусловлена ускоренным развитием цифровых технологий, которые усиливают поляризацию мнений и создают риски манипуляции. Алгоритмы социальных платформ определяют, какие новости и интерпретации получают приоритет, способствуя формированию «алгоритмического общественного мнения». Цель статьи – проанализировать роль киберпсихологии в процессах формирования общественного мнения в цифровой среде. Для достижения цели проведены синтез ключевых идей из литературы и анализ кейсов.

Трактовки киберпсихологии и основные риски. Киберпсихология представляет собой междисциплинарное направление, изучающее влияние цифровых технологий на психические процессы индивидов и коллективов в контексте взаимодействия с информационными экосистемами. Согласно одному из подходов, эта область фокусируется на анализе взаимодействия человеческой психики с биометрическими системами, где технологии, такие как интернет вещей (IoT), интегрируются с социальными механизмами, включая системы социального кредита, что может приводить к рискам цифрового тоталитаризма [7, с. 83]. В более позитивном ключе киберпсихология трактуется как субдисциплина, возникающая на пересечении традиционной психологии, позитивной психологии и дизайна, ориентированного на благополучие, с акцентом факторы, способствующие благополучию людей в процессе взаимодействия с технологиями и через них [2].

Цифровые платформы трансформируют процессы формирования общественного мнения. Алгоритмы социальных сетей определяют приоритетность контента, влияют на то, какие источники информации и интерпретации событий получают преимущество, что приводит к концепции «алгоритмического общественного мнения» как процесса и продукта, формируемого автоматизированными системами [3]. Социальные медиа становятся основным каналом доступа к информации, способствуют поляризации идей и созданию эхо-камер, в которых индивиды обмениваются мнениями в замкнутых сообществах [6, с. 294].

Существуют риски использования искусственного интеллекта (ИИ) в политической сфере, где генерация контента усиливает пропаганду и манипуляцию восприятием, особенно в периоды выборов [4, с. 290; 5, с. 171]. Исследования показывают: такие технологии влияют на восприятие честности политиков, а искренность выражения может превалировать над фактической точностью, способствуя распространению дезинформации [8, с. 383]. Киберпсихология необходима для понимания того, как алгоритмы ограничивают доступ к альтернативным взглядам и усиливают предубеждения [1].

Техники и подходы к формированию мнений. Один из ключевых подходов предполагает позитивную ориентацию, фокусирующуюся на процессах, которые способствуют благополучию индивидов через взаимодействие с технологиями, включая рефрейминг негативных аспектов и интеграцию с позитивной психологией для баланса между положительными и отрицательными сторонами технологий [2]. Другой подход подчеркивает роль алгоритмов в формировании общественного мнения как процесса и продукта, где платформы выступают в качестве «новых стражей информации», контролирующих поток контента и влияющих на его приоритетность и взаимодействие пользователей [3].

Третий подход сравнивает цифровой контент с историческими формами пропаганды, анализирует, как низкокачественный генерируемый искусственным интеллектом контент размывает границы между аутентичностью и манипуляцией в политическом дискурсе. Влияние осуществляется через технологии дипфейков и профилирования пользователей, когда ИИ манипулирует изображениями политиков и усиливает дезинформацию, что приводит к искажению общественного мнения в избирательных кампаниях [4, с. 291–292].

В киберпсихологии применяются техники, адаптированные к анализу цифровых данных. Методы, основанные на больших данных, предполагают анализ популяции пользователей социальных сетей. Учитываются критерии активности, самоидентификации и взаимодействия с контентом для измерения идеологической гомофилии и классификации новостей с использованием линейных SVM и метрик выравнивания [1].

В моделировании различаются подходы к честности и истине, с эмпирической проверкой на данных из месседжей политиков для выявления корреляций между стилем риторики и качеством источников [8, с. 384]. Риск-анализ, интегрированный в рамки экзистенциальных рисков, связанных с ИИ (X-Risk), подразумевает мониторинг системных угроз с использованием концепций устойчивости и выравнивания ИИ для оценки манипуляций в политических кампаниях [5, с. 170].

Биометрические информационные экосистемы способны оказывать влияние через интеграцию данных с социальными механизмами, например, системы кредита, где

технологии формируют восприятие реальности и могут приводить к тоталитарным практикам [7, с. 84]. В позитивном ключе влияние реализуется, если технологии способствуют позитивной трансформации, усиливая ментальные силы индивидов в цифровой среде [2].

Индонезийские исследователи отмечают, что социальные медиа стали платформой для обмена мнениями во время предвыборных дебатов, где алгоритмы ускоряют распространение контента, влияя на коллективные представления о кандидатах. Пользователи при взаимодействии с новостями в реальном времени формируют динамичные нарративы. Микротаргетинг усиливает влияние на решения, что подчеркивает необходимость разработки стратегий для повышения цифровой грамотности среди избирателей [6, с. 293].

Кейсы. В политических кампаниях 2024-2025 гг. ИИ использовался для генерации контента при развертывании мемов и визуалов, направленных на формирование общественного мнения. На выборах президента Румынии кандидаты применяли сгенерированные ИИ мемы с низкокачественными изображениями для создания образа аутентичности и продвижения националистических нарративов, обходя контроль традиционных СМИ. Визуалы, часто грубые и поляризующие, способствовали быстрому распространению идей через социальные платформы, усиливая влияние на избирателей за счет анонимности и вирусности. Так AI-slop, представляющий собой поток низкокачественного генерируемого контента, интегрируется в пропаганду, размывает грань между развлечением и манипуляцией, что привело к усилению поляризации в румынском обществе [4, с. 295–296].

Другой пример – угрозы дипфейк-технологий в создании и манипуляции образом политиков. В 2024 г. видео с Нэнси Пелоси, замедленное и отредактированное с помощью ИИ, создавало впечатление опьянения, что распространялось в социальных сетях и влияло на восприятие ее компетентности среди избирателей. Дипфейк с Бараком Обамой использовался для имитации оскорбительных заявлений, демонстрируя потенциал технологии для подрыва доверия к лидерам и формированию негативного общественного мнения [5, с. 173–174].

Рекомендации. Для минимизации рисков и усиления позитивного потенциала цифровых технологий можно предложить несколько мер. Внедрение систем мониторинга должно включать инструменты для выявления манипулятивного контента с акцентом на устойчивость платформ к дезинформации, что подразумевает разработку протоколов модерации, интегрирующих этические стандарты с человеческим надзором. Продвижение цифровой грамотности через образовательные инициативы позволит пользователям

распознавать искажения и оценивать источники, способствуя противодействию поляризации. Разработка дизайна технологий, ориентированного на благополучие, должна стимулировать позитивную трансформацию, включая алгоритмы, продвигающие разнообразный контент для снижения предубеждений. В политическом контексте это подразумевает регуляторные рамки для платформ, ограничивающие использование генерируемого контента в пропаганде, и обязательную маркировку такого контента.

Заключение. Цифровые технологии трансформируют общественное мнение в динамичный, алгоритмически обусловленный феномен. Искренность риторики часто превалирует над фактической точностью, а низкокачественный генерируемый контент размывает границы между аутентичностью и пропагандой. Это подчеркивает двойственную природу киберпсихологии: как дисциплины, диагностирующей риски тоталитаризма и дезинформации, так и предлагающей стратегии для усиления ментальных ресурсов индивидов. «Алгоритмическое общественное мнение» создает дилемму между открытостью систем и их прозрачностью. Без активного участия индивидов в формировании цифровых норм мнение рискует стать артефактом технологий, а не продуктом диалога. Рекомендации по мониторингу, цифровой грамотности и регуляции технологий направлены на баланс между инновациями и сохранением рациональности в коллективных процессах.

Список источников и литературы:

1. Bakshy E. Exposure to ideologically diverse news and opinion / E. Bakshy, S. Messing, L. A. Adamic [Электронный ресурс] // Science. 2015. Vol. 348. Is. 6239. PP. 1130-1132. URL: https://doi.org/10.1126/science.aaa1160 (дата обращения: 03.11.2025).

2. Fortuna P. Positive cyberpsychology as a field of study of the well-being of people interacting with and via technology [Электронный ресурс] // Front. Psychol. 2023. Vol .14-2023. URL: https://doi.org/10.3389/fpsyg.2023.1053482 (дата обращения: 05.11.2025).

3. Gandini, A., Keeling, S., & Reviglio, U. Conceptualising the ‘algorithmic public opinion’: Public opinion formation in the digital age [Электронный ресурс] / A. Gandini, S. Keeling, U. Reviglio // Dialogues on Digital Society. 2025. URL: https://doi.org/10.1177/29768640251323147 (дата обращения: 03.11.2025).

4. Gross E.-C. AI-Slop and Political Propaganda: The Role of AI-Generated Content in Memes and Influence Campaigns / E.-C. Gross, A. J. M. Colson [Электронный ресурс] // EON. 2025. Vol. 6. Is. 3. PP. 289-298. URL: https://clck.ru/3QFtoP (дата обращения: 05.11.2025).

5. Jańczuk H. Risks of Using Artificial Intelligence in Creating the Image of Politicians and in Electoral Campaigns [Электронный ресурс] // Ad Americam. Journal of

American Studies. 2024. Vol. 25. PP. 169-182. URL: https://doi.org/10.12797/AdAmericam.25.2024.25.10 (дата обращения: 06.11.2025).

6. Public Opinion Formation in the Digital Age: A Review of Literature / D. F. Sjoraida, B. W. K. Guna, A. R. Nugraha [et al.] [Электронный ресурс] // Indonesia Journal of Engineering and Education Technology (IJEET). 2024. Vol. 2. Is. 2. PP. 290-297. URL: https://journal.ataker.ac.id/index.php/ijeet/article/view/52/69 (дата обращения: 06.11.2025).

7. Vigariu M. G. The cyberpsychology of biometric information ecosystems. Sustainability or digital totalitarianism? [Электронный ресурс] / M. G. Vigariu, C.-A. Marin // Journal of Research and Innovation for Sustainable Society (JRISS). 2024. Vol. 6. Is. 1. PP. 83-87. URL: https://clck.ru/3QFwbU (дата обращения: 05.11.2025).

8. When liars are considered honest / S. Lewandowsky, D. Garcia, A. Simchon, F. Carrella [Электронный ресурс] // Trends in Cognitive Sciences. 2024. Vol. 28. Is. 5. PP. 383-385. URL: https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(24)00058-5 (дата обращения: 06.11.2025).

Илья Витальевич Дуев,
выпускник бакалавриата по программе «Политология и Мировая Политика», НИУ ВШЭ Санкт-Петербург,
E-mail: ivduev@edu.hse.ru

Ксения Олеговна Иванова,
выпускник бакалавриата по программе «Политология и Мировая Политика», НИУ ВШЭ Санкт-Петербург,
E-mail: koivanova_4@edu.hse.ru

Kseniia O. Ivanova,
Graduate of the Bachelor's degree program in Political Science and World Politics, National Research University of Higher School of Economics, Saint Petersburg,
E-mail: koivanova_4@edu.hse.ru

Ilya V. Duev,
Graduate of the Bachelor's degree program in Political Science and World Politics, National Research University of Higher School of Economics, Saint Petersburg,
E-mail: ivduev@edu.hse.ru

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ГОТОВНОСТЬ ЛЮДЕЙ МИРИТЬСЯ С НАРУШЕНИЕМ КОНФИДЕНЦИАЛЬНОСТИ ИХ ЛИЧНОЙ ИНФОРМАЦИИ СО СТОРОНЫ ГОСУДАРСТВА

FACTORS OF THE WILLINGNESS OF PEOPLE TO ACCEPT THE VIOLATION OF THEIR INFORMATION PRIVACY BY THE STATE

Аннотация. Настоящее время характеризуется расцветом киберпреступлений, а также других нарушений, которые осуществляются посредством использования информационных технологий. Данная работа исследует дилемму, с которой вынуждены сталкиваться современные государства: сохранять неприкосновенность частной жизни граждан или осуществлять усиленный контроль над их информацией для обеспечения безопасности? Это исследование утверждает, что при возможности манипулировать некоторыми индивидуальными факторами, связанными с ценностями граждан, государство способно внедрять более радикальные меры контроля для обеспечения безопасности при сохранении лояльности людей. Данная работа использует методы машинного обучения для выявления таких факторов и симуляции увеличения лояльности граждан.

Ключевые слова: кибербезопасность, машинное обучение, неприкосновенность частной жизни, конфиденциальность информации, киберпреступления, симуляция, взвешивание рисков, граждане, теория расчета приватности.

Abstract. Currently, cybercrimes are flourishing, as well as other violations that are carried out through the use of information technology. This work explores the dilemma that modern states are forced to face: to preserve the privacy of citizens or to exercise enhanced control over their information to ensure security? This study argues that if it is possible to manipulate some individual factors related to the values of citizens, the state is able to implement more radical control measures to ensure security while maintaining people's loyalty. This work uses machine learning methods to identify such factors and simulate an increase in citizen loyalty.

Key words: cybersecurity, machine learning, privacy, confidentiality of information, cybercrime, simulation, risk weighing, citizens, Privacy Calculus theory.

Современное время характеризуется расцветом информационных технологий. Это связано с развитием киберпреступлений, таких как кибермошенничество [7]. Кроме того, различные преступления, которые в конечном итоге совершаются в реальной жизни, также могут быть организованы онлайн. Это поднимает проблему кибербезопасности [7]. Государства начинают активно бороться с киберпреступлениями, терроризмом, который можно отследить через сеть, и другими угрозами [2], для чего власти необходимо максимально эффективно использовать существующую цифровую информацию. Однако, существует ряд правовых и этических ограничений, которые не позволяют государствам получить полный доступ ко всем ресурсам [2]. При этом, часто легче преодолеть юридические ограничения, чем этические.

Ученые, в основном, изучают, как балансировать между правовыми и этическими ограничениями и внедрять методы обеспечения безопасности [1]. Другие развивают эту логику, обсуждая роль общественного восприятия и доверия к правительству в принятии решений по контролю за технологиями и информацией [7]. Многие также упоминают терроризм как противовес правам человека в вопросах безопасности [6], оставляя открытым вопрос о том, какие из современных мер, связанных с доступом правительства к информации, являются приемлемыми и оправданными. Другие поддерживают дискуссию и упоминают распространение камер наблюдения в качестве одной из мер государственного информационного контроля [3].

В целом, исследователи изучают дилемму с разных точек зрения, но все сходятся во мнении, что даже при наличии реальной угрозы государство может столкнуться с сильным сопротивлением и недовольством своих граждан в связи с доступом властей к их личной информации. Большинство ученых пытаются найти баланс между мерами кибербезопасности и этическими вопросами со стороны разработанных и применяемых методов сбора и контроля информации [5], но лишь немногие рассматривают эту дилемму

с точки зрения приспособляемости человеческого мнения к данной проблеме. Иногда правительству действительно необходимо принять решительные меры безопасности, а завоевать расположение граждан может быть непросто. Из этого следует вопрос: какие факторы в наибольшей степени влияют на готовность людей мириться с нарушением их частной жизни государством?

Стоит заранее отметить, что на позицию людей по определенным вопросам могут влиять многие индивидуальные факторы в разном направлении и степени. Некоторые из них нелегко изменить, например, возраст или пол человека. Другие факторы могут быть более подвержены влиянию, например, доверие к правительству. Цель этого исследования – выяснить, существуют ли факторы, подвергаемые влиянию государства и которые важны для прогнозирования готовности граждан смириться с нарушением их неприкосновенности частной информации со стороны правительства. Важно также отметить, что прогнозирование негативного отношения к нарушению неприкосновенности является приоритетной задачей в данной работе. Это связано с тем, что в зависимости от негативной позиции граждан планируются возможные ограничения и риски от реализуемых мер. В этом случае гораздо важнее выявлять недовольных и управлять их мнением. Кроме того, наибольший интерес представляют факторы, на которые может повлиять государство.

Теория и переменные. Исходя из исследовательской задачи и вопроса, целевой переменной этой работы является готовность людей смириться с нарушением их частной (цифровой, информационной) жизни государством. В качестве основы для этой работы была использована теория расчета приватности [9], которая берет начало из поведенческой экономики, однако, в целом, способна объяснить, как человек мыслит и принимает решения [3]. Теория объясняет, как люди принимают решение о предоставлении другим личной информации, путем а) оценки выгод и рисков, б) контекстуальных факторов, таких как прошлый опыт или характеристики объекта запрашиваемой информации, и в) когнитивного процесса, включающего социальные нормы, которые разделяет человек [3].

На основе теории отобраны факторы для анализа:

а) Доход, удовлетворенность личным финансовым положением, семейное положение и количество детей - переменные, характеризующие возможные риски, связанные с предоставлением информации государству, или риски, связанные с ее сокрытием. Например, при соблюдении конфиденциальности у человека может возникнуть опасение, что государство вовремя не обнаружит террористов, которые могут представлять угрозу для детей;

б) Статус (мигрант или нет), доверие к государственным учреждениям и чувство безопасности - переменные, характеризующие прошлый опыт или особенности государства, запрашивающего доступ к информации;

в) Возраст и уровень образования - переменные, характеризующие когнитивные способности человека.

Для измерения факторов использованы данные последней, седьмой волны Всемирного исследования ценностей [4]. Целевая переменная рассчитана как взвешенное среднее значение мнений людей о возможности: а) разрешить правительству контролировать видеонаблюдение в общественных местах; б) разрешить правительству отслеживать электронную почту и интернет-коммуникации; в) разрешить правительству собирать информацию о людях без их ведома. Все три компонента связаны с позицией по вопросу о нарушениях конфиденциальности в сфере оцифрованной информации.

Анализ и результаты. Для анализа были выбраны методы логистической регрессии и случайного леса. После предварительной обработки данных были построены три модели с использованием случайного леса. В трех моделях использовался полный набор предикторов, но настройки параметров были разными: количество деревьев для построения и переменные, оставшиеся после итерации, варьировались. После этого были определены наиболее важные предикторы в модели, включая возраст, финансовую удовлетворенность и количество детей [4]. Используя наиболее важные переменные, была построена другая модель и рассчитана точность ее прогноза. Также были построены две логистические регрессии: с полным набором предикторов и с переменными, соответствующими последней модели случайного леса. Из всех моделей была выбрана модель с наивысшей точностью прогнозирования в тестовой выборке - логистическая регрессия со всеми предикторами. Точность этой модели составляет около 62,5%. Кроме того, важно отметить, что специфичность модели составила приблизительно 82%. Таким образом, модель умеренно хорошо предсказывает негативный класс.

Чтобы оценить важность характеристик, был построен график 1. Наиболее важными переменными являются в основном те, на которые трудно повлиять: возраст меняется с течением времени, количество детей и семейное положение зависят от семейных отношений и глубоко личных решений. При этом наиболее важным фактором оказалась переменная “доверие к государственным органам”, точнее, ее первый класс, означающий очень низкий уровень доверия. Этот фактор часто зависит от действий государства, когда мнение людей может меняться в зависимости от его действий. Таким образом, единственным значимым фактором, на который можно влиять, является доверие.

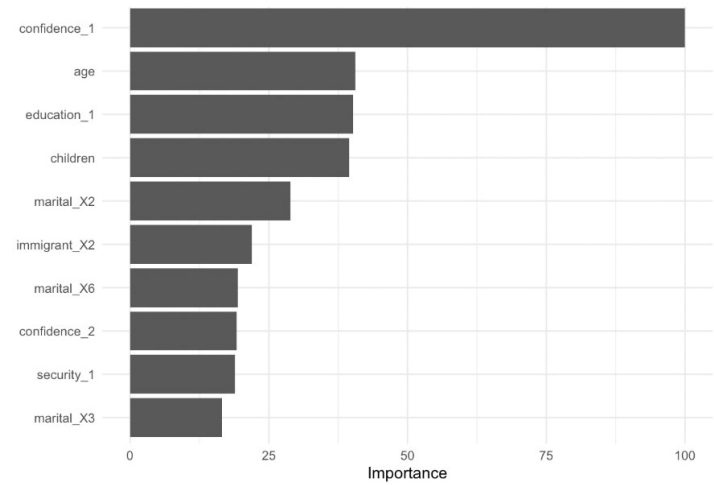


График 1. График важности переменных [4]

Последнее, что было сделано для того, чтобы увидеть, как с изменением доверия людей к государственным учреждениям будет происходить изменение в распределении классов целевой переменной - симуляция. Эксперимент заключался в следующем: 30% людей, которые ранее вообще не были уверены в государственных органах, перешли в группу тех, кто «достаточно уверен». Результат моделирования представлен на графике 2. Можно видеть, что, если 30% людей станут более уверенными в государственных структурах, больше людей будут считать допустимым нарушение государством конфиденциальности информации.

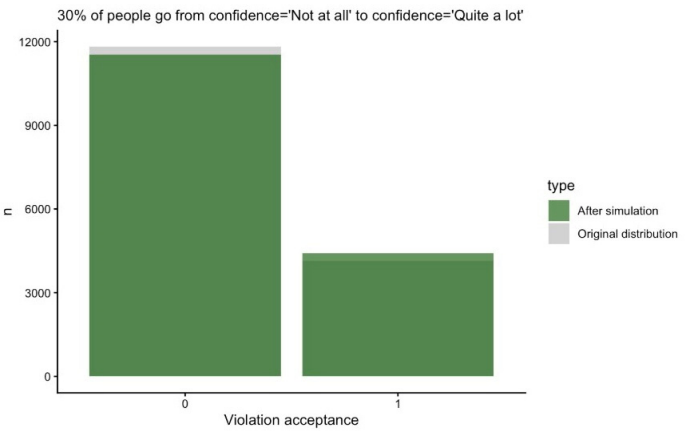


График 2. Результаты симуляции [4]

Интерпретируя полученные результаты, можно констатировать, что если государство повысит доверие граждан к своим основным институтам, больше граждан сочтут приемлемым для государства доступ к их личной информации. Таким образом, правительство сможет предсказать, насколько радикальные меры могут быть приняты для обеспечения безопасности при сохранении баланса с этическими соображениями.

Заключение. Анализ выделил наиболее важные факторы, влияющие на целевую переменную, а в результате симуляции было выявлено, что по мере роста доверия людей к государственным учреждениям люди будут более спокойно относиться к возможности государства вмешиваться в их личную информацию. Для будущих исследований в этой работе предлагается учитывать факторы на уровне страны в ходе анализа, поскольку они также могут влиять на целевую характеристику.

Список источников и литературы:

1. Allahrakha N. Balancing cyber-security and privacy: legal and ethical considerations in the digital age // Legal Issues in the digital Age. 2023. № 2. P. 78–121 (дата обращения: 20.09.2025).
2. Cuesta A., González-Villa J., Ortiz G., Alvear D. Anticipating public acceptance of anti-terrorism technologies in urban spaces: Insights from Czech Republic, Greece, and Spain // Safety Science. 2025. Vol. 189. Article 106888 (дата обращения: 20.09.2025).
3. Dienlin T. Privacy calculus: Theory, studies, and new perspectives // The Routledge handbook of privacy and social media. 2023. P. 70–79 (дата обращения: 20.09.2025).
4. Haerpfer C., Inglehart R., Moreno A., Welzel C., Kizilova K., Diez-Medrano J., Lagos M., Norris P., Ponarin E., Puranen B. World Values Survey Wave 7 (2017-2022) Cross-National Data-Set. Version 4.0.0. World Values Survey Association, 2022 (дата обращения: 20.09.2025).
5. Vanoni L. P. Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems // The Fragmented Landscape of Fundamental Rights Protection in Europe. 2018. P. 114–137 (дата обращения: 20.09.2025).
6. Prezelj I. Relationship Between Security and Human Rights in Counter-Terrorism // International Studies: Interdisciplinary Political and Cultural Journal. 2015. Vol. 17, No. 1. P. 145–158 (дата обращения: 20.09.2025).
7. Sharma A. Balancing National Security and Personal Privacy: Legal Implications of Encryption Backdoors in Global Cybersecurity Policy // Legal Studies in Digital Age. 2022. Vol. 1, No. 1. P. 53–67 (дата обращения: 20.09.2025).

8. Ünver H. A. Politics of digital surveillance, national security and privacy. Centre for Economics and Foreign Policy Studies, 2022 (дата обращения: 20.09.2025).
9. Wang T., Duong T. D., Chen C. C. Intention to disclose personal information via mobile applications: A privacy calculus perspective // International Journal of Information Management. 2016. Vol. 36, No. 4. P. 531–542 (дата обращения: 20.09.2025).

Элена Юрьевна Чуклина,
к.ю.н., научный сотрудник,
Федеральный исследовательский центр
Южный научный центр Российской академии наук,
E-mail: die_sehnsucht@mail.ru

Elena Iu. Chuklina,
Ph. D. in Law, Research Associate,
Federal Research Centre
Southern Scientific Centre of the Russian Academy of Sciences,
E-mail: die_sehnsucht@mail.ru

ОГРАНИЧЕНИЯ И ЗАПРЕТЫ ПОТРЕБЛЕНИЯ КОНТЕНТА В СЕТИ «ИНТЕРНЕТ»

RESTRICTIONS AND PROHIBITIONS ON CONTENT CONSUMPTION ON THE INTERNET

Аннотация. Статья посвящена обзору мер, ограничивающих потребление информации, размещенной в сети «Интернет». Подчеркивается неоднозначность блокировки и замедления зарубежных Интернет-платформ и необходимость изучения степени их негативного влияния на российских граждан. Автор анализирует норму, предусмотренную ст. 13.53 КоАП РФ, прогнозируя проблемы ее применения, связанные с выявлением и фиксацией факта правонарушения, доказыванием умысла и заведомого характера, расширительным описанием запрещенной к поиску информации экстремистского характера.

Ключевые слова: деструктивный контент, экстремизм, блокировка, Интернет, поиск информации, потребление контента, VPN.

Abstract. This article reviews measures restricting Internet consumption. It emphasizes the ambiguity of blocking and slowing down foreign Internet platforms and the need to study the extent of their negative impact on Russian citizens. The author analyzes the provision contained in Article 13.53 of the Code of Administrative Offenses of the Russian Federation, anticipating challenges in its application related to identifying and recording the offense, proving intent and deliberate nature, and providing a broad description of extremist information prohibited from being searched.

Key words: destructive content, extremism, blocking, Internet, information search, content consumption, VPN.

Информационно-психологическая безопасность. В стратегических документах Российской Федерации условно выделяются техническая и гуманитарная угрозы информационной безопасности, где первая означает атаки на критическую инфраструктуру, разведку, компьютерные преступления, второе – негативное воздействие на массовое и индивидуальное сознание. Соответственно в доктрине появилось понятие «информационно-психологическая безопасность», которая понимается как элемент информационной безопасности, представляющий собой защищенность граждан, отдельных групп и социальных слоев, массовых объединений людей и населения страны в целом от негативных информационно-психологических воздействий [3, с. 63]. Основными угрозами информационно-психологической безопасности россиян признаны искажение ключевых исторических фактов и образа России, пропаганда и оправдание криминальных и некриминальных деструктивных идей, милитаризация информационного пространства [5; 7; 11; 17].

Способы ограничения потребления контента. Противодействие перечисленным угрозам в сети «Интернет» осуществляется посредством блокировки Интернет-ресурсов и удаления материалов Роскомнадзором, привлечением к административной и уголовной ответственности за распространение деструктивной информации (ст.ст. 13.36, 13.37, 20.3 КоАП РФ, ст.ст. 205.2, 207.1-207.3 УК РФ и др.).

Вместе с тем запрет или замедление Интернет-ресурсов имеет и оборотную сторону – сужение возможностей пользователя на потребление контента. Если, например, блокировка доступа к видеозаписи, содержащей пропаганду террористической идеологии, несет исключительно полезный эффект, то блокировка целого видеохостинга с некоторой долей деструктивных видео может вызвать недовольство населения и полемику экспертов. Аналитики ВЦИОМ заявили, что «зумеры» и «миллениалы» негативно относятся к блокировкам Интернет-ресурсов, люди старше 58 лет относятся безразлично и положительно, спрогнозировав усложнение межпоколенческого диалога [4].

Западные Интернет-медиа действительно могут нести угрозу общественно-политической стабильности в России, в частности, как площадка для коммуникации участников протестных акций и митингов, призывов к убийству российских военнослужащих и т.п. [14, с. 3060; 19, с. 76].

Однако оценить степень негативного влияния указанных платформ довольно сложно. Ряд ученых, изучавших роль YouTube в формировании взглядов молодежи, пришли к выводам о высоком уровне критического мышления у пользователей этой платформы [15, с. 41], выраженном запросе у подростков на патриотизм в виде «мягкой

силы» государства [9, с. 19], небольшой популярности оппозиционных каналов [2, с. 578], предпочтении лицами от 18 до 34 лет политической сатиры серьезному политическому контенту [18, с. 114]. С приобретением Twitter[7] бизнесменом И. Маском изменилась информационная политика социальной сети, переименованной в X, позволяющая вытеснять неолиберальные нарративы антиWOKE-повесткой и освещением специальной военной операции с российской позиции. Ограничения работы Telegram в России объясняются борьбой с мошенниками [20], при этом стремительно растет объем мошенничества, совершаемого по сотовой связи [12], а Telegram по данным отчета Global Digital 2024: Russian Federation является любимой социальной сетью россиян [21].

С 1 сентября 2025 г. действует административная ответственность за поиск заведомо экстремистских материалов и получение доступа к ним, в том числе с помощью VPN (ст. 13.53 КоАП РФ). Министр цифрового развития, связи и массовых коммуникаций РФ М. Шадаев заявил, что данный запрет обеспечит ограничение распространения экстремистской информации без блокировки зарубежных платформ [8].

Возможные проблемы применения нормы, предусмотренной ст. 13.53 КоАП РФ. Сотрудники МВД России предупреждают о риске ложноположительных фиксаций системы DPI при анализе трафика VPN [1, с. 14]. М. Шадаев заявил, что передача поисковыми системами запросов пользователей правоохранительным органам не предусмотрена, привлекаться к ответственности будут «единицы» – организаторы экстремистских ячеек, последователи экстремисткой идеологии, которые уже находятся в поле зрения правоохранительных органов [8]. На данный момент оштрафован один гражданин за поиск информации о террористических организациях [16].

Критики закона справедливо задаются вопросом о доказывании умышленного поиска запрещенной информации. В диспозиции нормы ст. 13.53. КоАП РФ указано, что экстремистскими материалами являются те, которые включены в опубликованный федеральный список экстремистских материалов или указаны в п. 3 ст. 1 Федерального закона от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (далее – ФЗ № 114). На сайте Министерства юстиции Российской Федерации опубликовано около 5500 записей о материалах, признанных экстремистскими. Едва ли рядовой гражданин способен изучить и запомнить весь этот список.

Член комитета Государственной Думы России по информационной политике, информационным технологиям и связи А. Ткачев считает, что умысел доказывает преодоление всех преград, установленных государством к запрещенному контенту [13], что

[7] Бывший Twitter, соцсеть заблокирована в РФ.

в целом звучит рационально. Однако сложности доказывания могут возникнуть в случаях перманентного использования VPN или прокси-сервера из-за замедления YouTube или в связи с профессиональной деятельностью (ИТ-специалисты, стримеры).

Следует также заметить, что в диспозиции нормы содержится указание на п. 3 ст. 1 ФЗ № 114, согласно которому экстремистскими материалами являются, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, их выступления и изображения, труды, выступления, изображения руководителей групп, организаций или движений, признанных преступными Нюрнбергским трибуналом.

Данный запрет ставит под угрозу поиск информации в целях проведения исторических исследований, подготовки просветительских материалов и даже художественных произведений для образовательных учреждений, демонстрации по телевидению или в сети «Интернет», например, о деятельности Гестапо на территории нацистской Германии и оккупированных стран.

Заключение. Тренд на секьюритизацию Интернет-пространства будет охватывать все больше стран, усиливая изоляционизм и так культурно различающихся регионов мира. Однако концентрация исключительно на внешней угрозе может спровоцировать недовольство граждан и приток опасного контента на отечественные ресурсы, а также сократить возможности для применения «мягкой силы». В этой связи перед принятием решения о блокировке зарубежной Интернет-платформы необходимо оценить предполагаемые выгоду и издержки, степень ее негативного воздействия на общество, риск неконтролируемого перехода деструктивного контента на другие ресурсы. Норма, предусмотренная ст. 13.53. КоАП РФ, на данный момент выглядит не в полной мере ясной из-за отсутствия разъяснения механизма ее применения и угрозы необоснованного ограничения потребления контента в научных и просветительских целях.

Список источников и литературы:

1. Алексеева А.П., Анисимов А.П. Криминологическое исследование законодательных инициатив, усиливающих ответственность за поиск экстремистских материалов в сети «Интернет» // Вестник Волгоградской академии МВД России. 2025. № 3 (74). С. 11–18.

2. Бареев М.Ю., Качурина И.О. YouTube как фактор формирования протестного потенциала молодежи // Регионология. 2019. Т. 27. № 3. С. 572–587.

3. Баришполец В.А. Информационно-психологическая безопасность: основные положения // Радиоэлектроника. Наносистемы. Информационные технологии. 2013. Т. 5. № 2. С. 62–104.

4. Винокуров А. ВЦИОМ узнал отношение россиян к ограничению доступа к мессенджерам. Более половины молодых россиян негативно относятся к блокировкам интернет-ресурсов. [Электронный ресурс]. URL: https://www.rbc.ru/politics/07/11/2025/690d99ca9a7947e18cb44923?from=from_main_7 (дата обращения: 08.11.2025).

5. Военная доктрина Российской Федерации, утв. Указом Президента Российской Федерации от 05.02.2010 г. № 146. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/30593 (дата обращения: 03.07.2025)

6. Госдума приняла закон о штрафе за поиск в Сети экстремистских материалов. [Электронный ресурс]. URL: https://ria.ru/20250722/zakon-2030613896.html (дата обращения: 08.11.2025).

7. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента Российской федерации от 05.12.2016 № 646 // Собрание законодательства Российской Федерации от 12.12.2016 г. № 50 ст. 7074.

8. Закон о запрете поиска экстремистских материалов даёт возможность пока обойтись без блокировки зарубежных платформ - глава Минцифры РФ. [Электронный ресурс]. URL: https://www.interfax-russia.ru/moscow/news/zakon-o-zaprete-poiska-ekstremistskih-materialov-daet-vozmozhnost-poka-oboytis-bez-blokirovki-zarubezhnyh-platform-glava-mincifry-rf (дата обращения: 08.11.2025).

9. Касамара В.А., Сорокина А.А., Шилина А.Н. YouTube-блогеры как агенты политической социализации российских школьников // Вестник Московского университета. Серия 12. Политические науки. 2021. № 3. С. 7–20.

10. Клишас не видит риска массовых проверок за поиск экстремистских материалов. [Электронный ресурс]. URL: https://tass.ru/obschestvo/24596463 (дата обращения: 08.11.2025).

11. Концепция внешней политики Российской Федерации, утв. Указом Президента Российской Федерации от 31.03.2023 г. № 229 // Собрание законодательства Российской Федерации от 03.04.2023 г. № 14. ст. 2406.

12. Лазаренко Н., Хмурковская А. В России выросло количество телефонных мошеннических атак на 30%. На каждого жителя страны пришлось 35 звонков. [Электронный ресурс]. URL: https://www.rbc.ru/life/news/68f0bb449a79477dde472d54?ysclid=mhp62i9z1j808022710 (дата обращения: 07.11.2025).

13. Лисицына М., Химшиашвили М., Ситюков А., Пантелеев Д. Кому грозит поправка о штрафах за поиск экстремизма в интернете. [Электронный ресурс]. URL: https://www.rbc.ru/politics/16/07/2025/687759f79a794702368738b9 (дата обращения: 08.11.2025).

14. Макаренко К.М., Панкратова Л.С., Панкратов С.А. Трансформация гражданского протеста в современной России: выбор форм онлайн и офлайн активности // Вопросы политологии. 2021. Вып. 11 (75). Т. 11. С. 3055–3064.

15. Сиврикова Н.В. Системная оценка критичности мышления и особенностей медиапотребления студентов // Системная психология и социология. 2022. № 3 (43). С. 35–46.

16. Соколов К., Ларичева М. В России выписали первый штраф за поиск экстремистского контента. [Электронный ресурс]. URL: https://www.rbc.ru/politics/10/12/2025/6939684f9a7947ac893c161e?ysclid=mjlc8rs2xa806414196 (дата обращения: 24.12.2025).

17. Стратегия национальной безопасности Российской Федерации, утв. Указом Президента Российской Федерации от 02.07.2021 г. № 400 // Собрание законодательства Российской Федерации от 05.07.2021 г. № 27 (часть II) ст. 5351.

18. Темнова Л.В., Лапшина А.К. Динамика видеопредпочтений российской молодежи (на примере видеохостинга YouTube) // Вестник РУДН. Серия: Социология. 2021. Т. 21. № 1. С. 110–123.

19. Тимофеева А.П. Виртуальные средства медиакратии как акторы формирования угроз национальной безопасности Российской Федерации в современной гибридной войне // Русская политология. 2022. № 2 (23). С. 75–79.

20. Шокурова Е., Зыкина Т. В России начали ограничивать регистрацию в Telegram и WhatsApp. [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/31/10/2025/6903cec99a794758a0046cd9?ysclid=mhp5y4ld5h341414246 (дата обращения: 07.11.2025).

21. Global Digital 2024: Russian Federation. [Электронный ресурс]. URL: https://datareportal.com/reports/digital-2024-russian-federation (Accessed: 07.11.2025).

Софья Ивановна Фомина,
Студентка исторического факультета, направления «Политология» Иркутского государственного университета,
E-mail: fominasofa69213@gmail.com

Sofya Ivanovna Fomina,
Student of the Faculty of History, Department of Political Science, Irkutsk State University,
E-mail: fominasofa69213@gmail.com

ВЛИЯНИЕ АЛГОРИТМОВ НА ПОЛИТИЧЕСКИЕ ПРЕДПОЧТЕНИЯ

THE IMPACT OF ALGORITHMS ON POLITICAL PREFERENCES

Аннотация. Автором исследуется влияние алгоритмов социальных сетей и поисковых систем на формирование политических предпочтений пользователей. Рассмотрено, как алгоритмы, стремясь максимизировать вовлеченность, создают «информационные пузыри» и «эхо-камеры», что ведет к усилению политической поляризации и радикализации. Особое внимание уделяется роли дипфейков, чат-ботов и языковых моделей (на примере GPT-3) в распространении ложной информации.

Ключевые слова: искусственный интеллект, управление ИИ, влияние алгоритмов, политическая поляризация и радикализация, политическая сфера.

Abstract. The author explores the impact of social media and search engine algorithms on shaping users' political preferences. The article examines how algorithms, in an effort to maximize engagement, create "information bubbles" and "echo chambers," leading to increased political polarization and radicalization. Special attention is given to the role of deepfakes, chatbots, and language models (such as GPT-3) in spreading false information.

Key words: Artificial Intelligence, AI Governance, Algorithmic Influence, Political Polarization and Radicalization, Political Landscape.

Сегодня искусственный интеллект (ИИ) становится неотъемлемой частью нашей повседневности и применяется в медицине, науке, экономике и множестве других областей. Однако в статье будет затронута сфера, которая особенно остро реагирует на появление новых технологий и ощущает их воздействие наиболее глубоко – о политической сфере. Мы находимся в мире, который полностью окутан различной информацией. Социальные сети, новостные ленты, поисковые системы – все это стало частью нашей повседневной жизни, и мы даже не замечаем, как начинаем тонуть в этом потоке. Но за всем этим стоят различного рода алгоритмы, которые оказывают огромное влияние на массовое сознание, на то, как мы воспринимаем мир, и, что особенно важно, на наши политические предпочтения.

Алгоритм – последовательность вычислительных шагов, которые позволяют системе находить закономерности в данных и принимать решения. В отличие от обычных программ, где каждое действие жёстко прописано программистом, система ИИ, основанного на машинном обучении: его не учат напрямую готовым ответам, а дают правила и данные, из которых он выстраивает собственную модель поведения. Суть такого обучения и самих алгоритмов в том, чтобы выявлять закономерности между тем, что мы подаем на вход в сети интернет, и тем, что получаем на выходе из нее. Чем больше данных получает система на основе машинного обучения, тем лучше она решает поставленные перед ней задачи [1]. В современном обществе почти все публичные сферы управляются через алгоритмы, так как данные скрытые механизмы, интегрированы во множество цифровых платформ. С помощью данных механизмов и формируется множество взглядов на политику и политический процесс в целом. Все современные платформы (Google, Яндекс), а также социальные сети (Facebook[8], X[9], ВК) играют ключевую роль в организации доступа к информации у современного человека. Но зачастую люди даже не задумываются о том, насколько эта информация правдива. Таким образом, возрастает роль дипфейков и фэйков, которые негативно влияют на политическую сферу. Хотя алгоритмы и упорядочивают огромные объемы контента, определяют наиболее значимые источники, наиболее популярные темы и в конце формируют специальные ленты для каждого пользователя (все это делается на основе лайков, репостов и других действий). Несмотря на это, пользователь все равно может получать ту информацию, которой раньше не было, и, постепенно развивая ее в своей ленте, он способен полностью в нее поверить [4]. Именно поэтому алгоритмы социальных сетей – это сложные системы, которые отбирают и сортируют информацию, основываясь на ваших прошлых действиях. Их основная задача – не предоставить вам объективную картину мира, а заставить вас как можно дольше оставаться на платформе, ведь это напрямую влияет на прибыль компании от рекламы [3].

Некоторыми средствами распространения ложной политической информации могут быть чат-боты. В современном обществе, где люди часто чувствуют себя изолированными, виртуальные помощники перестали быть просто развлечением и стали выполнять роль компаньонов. Однако, начиная с 2018 года, данные программы стали вести себя как эмоциональные потребители, что сильно подорвало доверие к ним. Так было с передовой языковой моделью GPT.

[8] Принадлежит компании Meta, признанной экстремистской и запрещённой на территории РФ.
[9] Бывший Twitter, соцсеть заблокирована в РФ.

Как отмечают эксперты, алгоритмы на базе GPT-3 склонны усваивать и распространять негативный контент, будь то агрессивные высказывания, слухи или ложная информация. Получается, что проблема не только в самих разработчиках и их творениях, но и в том, с кем эти программы общаются после выхода в онлайн. Например, в сфере разработки ИИ существует проблема жестокого обращения с ботами: некоторые пользователи вымещают на них свою агрессию, а программы, в свою очередь, начинают копировать и воспроизводить такое же враждебное поведение [2]. А если подобное жестокое обращение будет идти в адрес бота, который направлен на политику, то распространение различного рода негативной информации среди масс не избежать, так как многие люди зачастую очень критично оценивают действия текущей власти.

Одним из негативных последствий работы алгоритмов может выступать алгоритмическая поляризация и радикализация общества. Данные термины представляют собой определенные концепции, связанные с использованием алгоритмов в социальных сетях, которые, по мнению исследователей, способствуют усилению политической поляризации и распространению экстремального контента. Поляризация действует таким образом: современные цифровые платформы, стремясь удержать внимание пользователей, активно используют алгоритмические системы рекомендаций. Подобные системы, анализируя предпочтения и прошлые взаимодействия пользователя, подбирают контент, который с высокой вероятностью вызовет интерес и обеспечит вовлечённость. Однако такой подход зачастую приводит к формированию так называемых «информационных пузырей» или «эхо-камер», где пользователи сталкиваются преимущественно с информацией, подтверждающей их существующие взгляды. Такая избирательная подача информации оказывает существенное влияние на восприятие окружающей действительности человека. В частности, она усиливает действие когнитивных искажений сознания человека, таких как предвзятость, персонализация, чрезмерное обобщение и многое другое. В результате пользователи оказываются в замкнутом цикле, где их взгляды постоянно подкрепляются потоком однородных новостей, мнений и аналитических материалов, делая их менее восприимчивыми к альтернативным точкам зрения и критическому осмыслению информации [1].

В современном цифровом пространстве, характеризующемся быстрым ростом объемов информации, алгоритмы рекомендательных систем играют ключевую роль в формировании информационного поля пользователя. Однако все чаще поднимается вопрос о потенциальном влиянии алгоритмов на процесс радикализации, определяемого как постепенное принятие экстремистских взглядов и убеждений. Существуют опасения, что алгоритмы, оптимизированные для максимизации вовлеченности пользователей, отдают

предпочтение контенту, вызывающему сильные эмоциональные реакции. Примером задействования подобного механизма могут служить алгоритмы рекомендаций YouTube или TikTok. Наблюдения показывают, что пользователи, начинающие просмотр с нейтрального контента, например, видео о здоровом питании, постепенно перенаправляются к более экстремальным темам, таким как теории заговора о плоской Земле или псевдонаучные «откровения инсайдеров». Подобный процесс, характеризующийся постепенным и незаметным для пользователя смещением в сторону радикального контента, получил название «спирали радикализации» [6].

Сильное влияние таких концепций привело к тому, что в некоторых странах хотят вводить ограничения на законодательном уровне. Так, например, Франция, Греция и Испания обсуждают введение обязательных возрастных ограничений для пользователей социальных сетей, включая Facebook[10] и X[11]. После принятия закона все устройства, которые имеют доступ в интернет, должны будут снабжаться функцией проверки возраста. Кроме того, от компаний, владеющих социальными сетями, будут требовать, чтобы их дизайн учитывал возраст пользователей, а также, чтобы они убрали функции, которые могут сильно затягивать или навязчиво привлекать внимание. Подобные меры касаются всплывающих окон, настроенного под вас контента и видео [5].

Заключение. Влияние алгоритмов на формирование политических предпочтений представляет собой сложный и многогранный процесс. С одной стороны, алгоритмы упрощают доступ к информации и персонализируют контент, с другой – они создают «информационные пузыри», способствуют поляризации общества и распространению дезинформации. А стремление цифровых платформ к максимизации вовлеченности пользователей зачастую приводит к возникновению у людей радикальных мыслей благодаря эмоционально заряженному и неправильному контенту. Именно поэтому становится очевидно, что дальнейшее развитие алгоритмов требует не только технологических улучшений, но и этической регуляции, а также повышения цифровой грамотности у пользователей.

Список литературы и источников:

1. Алгоритмы ИИ: понятное объяснение простым языком - виды, задачи, выбор подхода // NeuroToday : [сайт]. – URL: https://golnk.ru/kJdVW (дата обращения:05.11.2025).

2. Гундарова Л. Чат-боты: дьявол кроется в деталях / Гундарова Л. // Звезда : [сайт]. – URL: https://golnk.ru/vwA8x (дата обращения: 05.11.2025).

[10] Принадлежит компании Meta, признанной экстремистской и запрещённой на территории РФ.
[11] Бывший Twitter, соцсеть заблокирована в РФ.

3. Как алгоритмы социальных сетей ведут к радикализации: механизмы влияния на сознание молодежи // Работаем, брат : [сайт]. – URL: https://golnk.ru/7gpNX (дата обращения: 05.11.2025).

4. Косоруков А. А. Алгоритмы поисковых машин и социальных сетей как фактор становления цифровой публичной сферы / Косоруков А. А. // КиберЛенинка : [сайт]. – URL: https://cyberleninka.ru/article/n/algoritmy-poiskovyh-mashin-i-sotsialnyh-setey-kak-faktor-stanovleniya-tsifrovoy-publichnoy-sfery (дата обращения: 05.11.2025).

5. Натин А. Три страны Европы могут ограничить доступ к соцсетям по возрасту / Натин А. // Газета.ru : [сайт]. – URL: Три страны Европы могут ограничить доступ к соцсетям по возрасту // Газета.ru. URL: https://golnk.ru/6npk0 (дата обращения: 5.11.2025). (дата обращения: 05.11.2025).

6. Смоляков А. Алгоритм ненависти. Как социальные сети приводят к радикализации общества / Смоляков А. // Беларуская ассоциация журналистов : [сайт]. – URL: https://golnk.ru/NQBLR (дата обращения: 05.11.2025).

Секция С3
«Цифровые общества и трансформация социально-гуманитарной среды»

Елизавета Сергеевна Санникова,
студент 2 курса,
направления Политология,
Иркутский Государственный Университет,
E-mail: yelizaveta.sannikova.28@mail.ru

Elizaveta S. Sannikova,
2nd year student of political science
At Irkutsk State University,
E-mail: yelizaveta.sannikova.28@mail.ru

СОЦИАЛЬНЫЕ ПОСЛЕДСТВИЯ ВНЕДРЕНИЯ МЕТАВСЕЛЕННОЙ

SOCIAL CONSEQUENCES OF THE INTRODUCTION OF METAVERSE

Аннотация. В статье рассматриваются социальные последствия развития и внедрения метавселенной как нового медиафеномена. На основе синтеза данных выявлены ключевые вызовы, затрагивающие социальное взаимодействие, психологическое здоровье и экономические отношения. Проведенный анализ показывает, что внедрение метавселенной требует создания этических и правовых рамок, призванных снизить системные угрозы и способствовать реализации конструктивного потенциала технологии.

Ключевые слова: метавселенная, социальные последствия, развитие, внедрение, вызовы.

Abstract. The article examines the social consequences of the development and implementation of the metaverse as a new media phenomenon. Based on the data synthesis, key challenges affecting social interaction, psychological health, and economic relations have been identified. The analysis suggests that the introduction of the metaverse requires the creation of an ethical and legal framework designed to reduce systemic threats and contribute to the realization of the constructive potential of technology.

Key words: metaverse, social consequences, development, implementation, challenges.

Метавселенная – цифровая платформа, основанная на технологиях смешанной реальности (MR), которая интегрирует виртуальные и физические объекты в единое гибридное пространство. В отличие от виртуальной реальности (VR), создающей иммерсивную искусственную среду, и дополненной реальности (AR), которая накладывает цифровые элементы на реальный мир, метавселенная обеспечивает их глубокую конвергенцию. Данная платформа предоставляет возможность взаимодействовать с виртуальными объектами и другими пользователями в настоящем времени [1, с. 222].

Стремительный рост технологий метавселенной несет не только технические, но и фундаментальные социальные вопросы. С одной стороны, метавселенная открывает уникальные возможности: стирание географических барьеров, новые формы творчества и экономики, а также изменения в сфере образования. С другой стороны, внедрение данной технологии имеет множество рисков: углубление цифрового неравенства, угрозы конфиденциальности данных, а также психологические проблемы.

Развитие метавселенной несет в себе ряд положительных последствий для общества. Прежде всего, способствует упрочнению и обогащению социальных связей, поскольку коммуникация приобретает новые формы взаимодействия, способствуя установлению контактов и сплочению обществ по интересам, независимо от географических границ [3, с. 176]. Кроме того, значительный потенциал метавселенная раскрывает в развитии образовательной и научной сфер, создавая возможности для повышения доступности и качества образования, а также для формирования международных научных связей, работающих в совместных виртуальных пространствах. Параллельно открываются новые формы досуга и культурного обмена, включая виртуальный туризм, доступ к культурным ценностям и получение уникального опыта. Формируются широкие экономические возможности, связанные со становлением виртуальной экономики, созданием новых ниш для бизнеса и рынков труда, ориентированных на разработку и владение цифровыми активами [5, с. 10-12].

Несмотря на положительный эффект, внедрение метавселенной имеет серьезные вызовы, требующих комплексного осмысления. Наиболее непосредственные риски метавселенной связаны с воздействием на личность и общество. Возникает опасность цифровой изоляции и киберзависимости. Чрезмерное погружение в виртуальную реальность может привести к забвению реального мира, нарушению процессов социализации, особенно среди детей и подростков, и формированию патологической зависимости [2, с. 21]. Метавселенная также рискует не сократить, а усилить социальное и экономическое неравенство. Цифровой разрыв углубляется: доступ будет зависеть от дорогостоящего оборудования, цифровых навыков и скорости интернета, создавая новую форму технологического расслоения. Из-за ограниченных возможностей для стабильного заработка экономическое неравенство возрастет, разделяя общество на «цифровую элиту» и всех остальных [4, с. 15-16]. Еще одной ключевой проблемой является утрата конфиденциальности данных. Функционирование метавселенной как платформы, обладающей возможностью сбора и обработки биометрических данных, порождает системную угрозу приватности и создает предпосылки для нарушения правовых норм в области защиты персональных данных [1, с. 225]. Метавселенная также может стать средой

для распространения дезинформации, мошенничества и организации преступной деятельности, что создает новые киберриски.

Заключение. Метавселенная представляет собой не просто технологический прорыв, а сложный социотехнический феномен, несущий в себе двойственный потенциал. С одной стороны, она открывает возможности для преодоления географических барьеров, развития образования, науки, экономики и социального взаимодействия, создавая новую среду для творчества, досуга и глобальной кооперации. С другой стороны, ее развитие связано с рисками, которые требуют системного подхода. Угрозы цифрового неравенства, киберзависимости, приватности и новых форм преступности ставят перед обществом серьезные вызовы. Поэтому успешная интеграция метавселенной в жизнь общества возможна лишь при условии осознанного и сбалансированного подхода ко всем аспектам данного многогранного явления.

Список источников и литературы:

1. Ангел О. Ю. Метавселенная как новый медиафеномен социума: перспективы создания и социальные последствия / О. Ю. Ангел. – Текст : электронный // Государственное и муниципальное управление. Ученые записки. – 2023. – № 3. – С. 221-226. – URL: https://cyberleninka.ru/article/n/metavselennaya-kak-novyy-mediafenomen-sotsiuma-perspektivy-sozdaniya-i-sotsialnye-posledstviya (дата обращения: 10.11.2025).
2. Ваторопин А. С. Ваторопин С. А. Тепляков И. И. Чевтаева Н. Г. Метавселенная: перспективы создания и социальные последствия / А. С. Ваторопин, С. А. Ваторопин, И. И. Тепляков, Н. Г. Чевтаева. – Текст : электронный // Теория и практика общественного развития. – 2022. – № 4 (170). – С. 19-25. – URL: https://cyberleninka.ru/article/n/metavselennaya-perspektivy-sozdaniya-i-sotsialnye-posledstviya (дата обращения: 10.11.2025).
3. Ильинская, Е. А. Социально-культурный феномен виртуальных сообществ / Е. А. Ильинская, И. А. Петрова // Общество: философия, история, культура. – 2025. – № 6 (134). – С. 173-178. – DOI 10.24158/fik.2025.6.22. – EDN JBZEPU.
4. Струнин Д. А. Метавселенная: влияние виртуальных миров на современный бизнес и общество / Д. А. Струнин. – Текст : электронный // Молодой ученый. – 2025. – № 7 (558). – С. 15-16. – URL: https://moluch.ru/archive/558/122677 (дата обращения: 10.11.2025).
5. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права / И. А. Филипова. – Текст : электронный // Journal of Digital Techonologies and Law. – 2022. – № 1. – С. 7-32. –URL: https://cyberleninka.ru/article/n/sozdanie-metavselennoy-posledstviya-dlya-ekonomiki-sotsiuma-i-prava (дата обращения: 10.11.2025).

Захар Евгеньевич Матвейчук,
студент 3 курса, направление «Международные отношения»,
исторический факультет, кафедра мировой истории
и международных отношений,
Иркутский государственный университет;
стажер Школы МИБ,
E-mail: zakhar_2026@internet.ru

Zakhar E. Matveichuk,
3rd year student, International Relations,
Faculty of History, Department of World History
and International Relations,
Irkutsk State University;
Trainee at the School of IIS,
E-mail: zakhar_2026@internet.ru

ИИ КАК ИНСТРУМЕНТ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ В РАМКАХ ШОС: КЕЙС НАРКОТРАФИКА В «ЗОЛОТОМ ТРЕУГОЛЬНИКЕ»

AI AS A TOOL FOR REGIONAL SECURITY WITHIN SCO: THE GOLDEN TRIANGLE DRUG TRAFFICKING CASE

Аннотация. В тезисах анализируется потенциал внедрения технологий искусственного интеллекта (ИИ) в деятельность Шанхайской организации сотрудничества (ШОС) для противодействия наркоугрозе. Рассматривается трансформация наркобизнеса в «Золотом треугольнике», связанная с переходом на синтетические наркотики и цифровизацией криминальных сетей. Выделены ключевые направления использования ИИ: предиктивная аналитика, спутниковый мониторинг, анализ данных Darknet. Особое внимание уделено успешному опыту Китая в использовании цифровых платформ общественной безопасности и возможности масштабирования этого опыта на пространство ШОС. Обозначены политические барьеры и предложены рекомендации по созданию пилотных проектов под эгидой РАТС ШОС.

Ключевые слова: ШОС, искусственный интеллект, наркотрафик, Золотой треугольник, региональная безопасность, РАТС, цифровая трансформация, опыт Китая.

Abstract. The thesis analyzes the potential of implementing artificial intelligence (AI) technologies into the activities of the Shanghai Cooperation Organization (SCO) to counter the drug threat. The transformation of drug trafficking in the "Golden Triangle", associated with the shift to synthetic drugs and the digitalization of criminal networks, is considered. Key areas of AI

application are highlighted: predictive analytics, satellite monitoring, and Darknet data analysis. Particular attention is paid to China's successful experience in using digital public security platforms and the possibility of scaling this experience to the SCO space. Political barriers are identified, and recommendations for pilot projects under the SCO RATS are proposed.

Key words: SCO, artificial intelligence, drug trafficking, Golden Triangle, regional security, RATS, digital transformation, China's experience.

Трансформация угроз и необходимость технологического ответа. Современная архитектура безопасности в Евразии испытывает системное давление со стороны трансформирующегося наркобизнеса. Регион «Золотого треугольника», исторически являвшийся центром производства опиатов, превратился в глобальный хаб синтетических наркотиков. По данным международных наблюдателей, Мьянма вышла в мировые лидеры по производству опия, однако главную угрозу представляет взрывной рост производства метамфетамина и других синтетических веществ [5].

Ключевой проблемой становится высокая технологическая адаптивность криминальных сетей. Наркосиндикаты активно используют цифровые инструменты: от шифрованных коммуникаций до криптовалют и сложной логистики поставок прекурсоров [9]. В этих условиях методы физического перехвата демонстрируют ограниченную эффективность. Шанхайская организация сотрудничества (ШОС) нуждается в качественном обновлении инструментария Региональной антитеррористической структуры (РАТС) за счет внедрения технологий искусственного интеллекта (ИИ).

Потенциал ИИ-решений и опыт КНР. Искусственный интеллект способен перевести борьбу с наркотрафиком из реактивной плоскости в проактивную. При этом ШОС не нужно создавать технологии с нуля – целесообразно опираться на передовой опыт государств-членов, прежде всего Китая. В настоящий момент КНР уже реализует концепцию «умной общественной безопасности», используя цифровые платформы (Digital Public Security Platforms), которые интегрируют ИИ и блокчейн для отслеживания незаконных финансовых потоков и киберугроз [12].

Можно выделить три вектора применения ИИ, релевантных для масштабирования в рамках ШОС:

1. Предиктивная аналитика (Big Data). По аналогии с китайскими системами анализа данных, единая платформа ШОС могла бы обрабатывать таможенные декларации и отчеты об изъятиях для выявления неочевидных закономерностей. Алгоритмы способны прогнозировать маршруты трафика и места создания нарколабораторий на основе косвенных признаков (например, аномального импорта химикатов) [7].

2. Спутниковый мониторинг (Computer Vision). Автоматизированный анализ спутниковых снимков позволяет контролировать труднодоступные горно-лесистые районы Мьянмы и Лаоса. ИИ эффективно распознает тепловые сигнатуры лабораторий и изменения ландшафта, что уже применяется Китаем при мониторинге приграничных зон.

3. Мониторинг теневого сегмента Интернета и финансов. Использование обработки естественного языка (NLP) и алгоритмов финразведки позволяет выявлять сбыт в Darknet и паттерны отмывания денег через криптовалюты [4; 9].

Политические и институциональные барьеры. Несмотря на наличие готовых технологических решений у Китая, их трансфер на уровень ШОС сталкивается с вызовами. *Во-первых,* это проблема цифрового суверенитета. Обмен чувствительной оперативной информацией для обучения нейросетей требует беспрецедентного уровня доверия [3]. Существует риск восприятия доминирования китайских технологических стандартов как угрозы национальной безопасности других участников. *Во-вторых,* технологический разрыв. Государства ШОС находятся на разных стадиях цифрового развития. Без гармонизации законодательства и подготовки кадров внедрение сложных ИИ-систем в менее развитых странах-членах будет неэффективным.

Заключение. Для реализации технологического потенциала ШОС необходимо:

1. Запуск пилотного проекта под эгидой РАТС. Использовать опыт КНР для создания тестовой системы мониторинга транзакций прекурсоров. Это позволит отработать протоколы обмена данными без критических рисков для суверенитета.

2. Трансфер компетенций. Создание на базе ШОС Центра компетенций, где специалисты из стран-участниц смогут обучаться работе с «умными» системами анализа данных, сокращая технологический разрыв.

3. Унификация стандартов. Разработка модельных актов, регулирующих использование ИИ в правоохранительной сфере, что создаст правовой фундамент для интеграции национальных систем.

Список источников и литературы:

1. Ван Чаоцин. Международное сотрудничество в области безопасности между ШОС и ОДКБ / Ван Чаоцин // Политология. – С. 123–127. – URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-oblasti-bezopasnosti-mezhdu-shos-i-odkb (дата обращения: 13.11.2025).

2. В Астане подписан протокол о взаимопонимании между РАТС ШОС и Секретариатом ОДКБ [Электронный ресурс] // Исполнительный комитет РАТС ШОС. – 2011. – URL: https://ecrats.org/ru/press/news/188/ (дата обращения: 13.11.2025).

3. Гордиенко, Д. В. Шанхайская организация сотрудничества как площадка для диалога по вопросам региональной безопасности / Д. В. Гордиенко // Национальные интересы: приоритеты и безопасность. – 2015. – № 37 (322). – С. 44–66. – URL: https://cyberleninka.ru/article/n/shanhayskaya-organizatsiya-sotrudnichestva-kak-ploschadka-dlya-dialoga-po-voprosam-regionalnoy-bezopasnosti (дата обращения: 13.11.2025).

4. Как технологии оказались секретным оружием в эпицентре азиатской наркоторговли [Электронный ресурс] // Police1. – 2024. – URL: https://www.police1.com/police-products/narcotics-identification/articles/how-technology-proved-to-be-a-secret-weapon-in-the-epicenter-of-the-asian-drug-trade-dQ0DyAKEU6AMYCii/ (дата обращения: 13.11.2025).

5. Рост производства и незаконного оборота синтетических наркотиков из «Золотого треугольника» [Электронный ресурс] // УНП ООН. – 2025. – URL: https://www.unodc.org/unodc/en/press/releases/2025/May/rise-in-production-and-trafficking-of-synthetic-drugs-from-the-golden-triangle--new-report-shows.html (дата обращения: 13.11.2025).

6. Талибы просят ШОС помочь в борьбе с производством наркотиков в стране [Электронный ресурс] // Афганистан.Ру. – 2006. – URL: https://afghanistan.ru/doc/9291.html (дата обращения: 13.11.2025).

7. ШОС активизирует сотрудничество в борьбе с незаконным оборотом наркотиков [Электронный ресурс] // DKNews.kz. – 2022. – URL: https://dknews.kz/ru/shelkovyy-put/283206-shos-aktiviziruet-sotrudnichestvo-v-borbe-s (дата обращения: 13.11.2025).

8. ШОС и ОДКБ проведут в 2020 году совместную антинаркотическую операцию [Электронный ресурс] // ТАСС. – 2020. – URL: https://tass.ru/mezhdunarodnaya-panorama/8819911 (дата обращения: 13.11.2025).

9. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia [Электронный ресурс] // UNODC Technical Policy Brief. – 2024. – January. – URL: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2024/2024_UNODC_Casinos_Report_-_Policy_Brief_final.pdf (дата обращения: 13.11.2025).

10. International Narcotics Control Strategy Report: Volume I [Электронный ресурс] // US Dept of State. – 2025. – URL: https://www.state.gov/wp-content/uploads/2021/02/International-Narcotics-Control-Strategy-Report-Volume-I-FINAL-1.pdf (дата обращения: 13.11.2025).

11. Khondakar, H. K. Golden Triangle to Bangladesh: Regional Analysis of ATS Sources, Trafficking Routes and Kingpin Involved, and Role of Regional Organizations / H. K. Khondakar // International Research in Social Sciences. – 2024. – Vol. 2, № 1. – P. 1–37. – DOI: 10.20849/irss.v2i1.1407 (дата обращения: 13.11.2025).

12. China’s public security vision: Global Governance Initiative in action [Электронный ресурс] // CGTN. – 2024. – 16 Sept. – URL: https://news.cgtn.com/news/2024-09-16/China-s-public-security-vision-Global-Governance-Initiative-in-action-1GHS62bBPhS/p.html (дата обращения: 13.11.2025).

Мария Константиновна Водопьянова,
Владислава Борисовна Дрюпина,
студенты 4 курса Института прокуратуры
Уральского государственного юридического
университета имени В.Ф. Яковлева,
E-mail: maria22022004@mail.ru;
vladislavadryupina@yandex.ru

Maria Kon. Vodopyanova,
Vladislava Bor. Drupina,
4th year students of the Institute of Public Prosecutor's Office
Ural State Law University named after V.F. Yakovlev,
E-mail: maria22022004@mail.ru;
vladislavadryupina@yandex.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МУЗЕЕВ: ОТ УЯЗВИМОСТЕЙ К СИСТЕМНОЙ ЗАЩИТЕ КУЛЬТУРНОГО НАСЛЕДИЯ

INFORMATION SECURITY OF MUSEUMS: FROM VULNERABILITIES TO SYSTEMIC PROTECTION OF CULTURAL HERITAGE

Аннотация. В статье исследуются актуальные вызовы и современные подходы к обеспечению информационной безопасности в музейной сфере. Рассматривается диалектика технологического прогресса, когда цифровизация, с одной стороны, открывает новые возможности, а с другой –расширяет поверхность для кибератак, что иллюстрируется конкретными примерами. Доказано, что формирование целостной, проактивной архитектуры кибербезопасности, основанной на международных стандартах и междисциплинарном подходе, является стратегическим приоритетом для сохранения культурного наследия в условиях перманентной цифровой трансформации.

Ключевые слова: информационная безопасность музеев, кибербезопасность культурного наследия, защита данных, цифровые угрозы, международные стандарты, цифровая трансформация.

Abstract. The article examines current challenges and modern approaches to ensuring information security in the museum sector. The article considers the dialectic of technological progress, when digitalization, on the one hand, opens up new opportunities, and on the other, expands the surface for cyber attacks, which is illustrated by specific examples. It is proved that the formation of a holistic, proactive cybersecurity architecture based on international standards and an interdisciplinary approach is a strategic priority for the preservation of cultural heritage in the context of permanent digital transformation.

Key words: information security of museums, cybersecurity of cultural heritage, data protection, digital threats, international standards, digital transformation.

Базовые концепции информационной безопасности. Формирование системы информационной защиты музеев требует четкого понимания базовой категории – безопасности. В своем исходном значении *(от лат. securitas)* этот термин описывает ситуацию, при которой жизненно важные интересы общества, государства и личности защищены от потенциального ущерба, источником которого могут выступать различные сферы человеческой деятельности.

Применительно к информационной сфере безопасность данных предполагает их сохранность от любых негативных для владельца последствий: утечки (подрыв конфиденциальности), модификации (утрата целостности), блокирования (ограничение доступности) или незаконного распространения [1, с. 9]. Таким образом, обеспечение безопасности информации достигается через внедрение комплексной системы ее защиты, где эти два понятия являются взаимосвязанными и взаимообусловленными.

Следовательно, информационная безопасность представляет собой комплексный процесс, нацеленный на защиту информационных ресурсов и поддерживающей инфраструктуры от деструктивных воздействий, способных нанести ущерб их конфиденциальности, целостности и доступности. Ключевая задача этой деятельности – системное прогнозирование угроз, их профилактика и минимизация возможного урона. Для музеев, выполняющих функцию хранителей культурного кода нации, построение такой защитной системы является не просто технической необходимостью, а стратегическим приоритетом. Грамотный подход, предполагающий поэтапную имплементацию защитных механизмов, позволяет достичь высокого уровня устойчивости без критической нагрузки на бюджет.

Кейс-анализ: системные уязвимости Лувра. Ситуация, связанная с системами защиты музея Лувр, представляет собой наглядный пример системных упущений в области обеспечения информационной безопасности [3]. Согласно данным, опубликованным в СМИ, в 2014 г. одна из критически важных подсистем, видеонаблюдение, была защищена крайне ненадежным паролем «Louvre», что является прямым нарушением базового принципа сложности учетных данных. Более того, аналогичная ситуация наблюдалась и в программном обеспечении, разработанном компанией Thales, где в качестве кода доступа также использовалось название фирмы-производителя. Подобная практика демонстрирует пренебрежение к фундаментальным требованиям политики парольной защиты, сводя на нет эффективность даже технологически продвинутых систем.

Дополнительным фактором уязвимости выступило использование морально устаревшей программной платформы. Хранение и обработка критических данных безопасности осуществлялись на операционной системе Windows Server 2003, которая к тому времени уже не поддерживалась разработчиком. Отсутствие регулярных обновлений и исправлений уязвимостей создавало предпосылки для потенциального несанкционированного доступа, поскольку известные программные бреши в такой среде не могли быть устранены. Это указывает на серьезные просчеты в управлении ИТ-инфраструктурой и несвоевременную модернизацию ключевых компонентов. Итогом реализации этих рисков стало ограбление, произошедшее в октябре, в ходе которого была похищена коллекция королевских драгоценностей стоимостью 88 млн евро. Хотя прямая причинно-следственная связь между конкретными уязвимостями и инцидентом официально не установлена, совокупность выявленных недостатков формирует комплексную картину недостаточного уровня защищенности. Данный прецедент подчеркивает, что для учреждений, подобных Лувру, безопасность должна быть не набором разрозненных технических мер, а целостной, постоянно актуализируемой стратегией, интегрированной во все операционные процессы.

Вызовы внедрения искусственного интеллекта в музейной сфере. Проблемы технологической уязвимости, аналогичные случаю с Лувром, проявляются и в ином аспекте цифровизации музейного пространства – сфере внедрения искусственного интеллекта. Яркой иллюстрацией консервативного подхода является позиция директора ГМИИ им. Пушкина Е. Лихачёвой, заявившей о полном отказе учреждения от использования ИИ в текущих условиях [6].

Основной причиной названа низкая достоверность генерируемого контента, обусловленная, по её мнению, катастрофическим состоянием цифровой информационной среды. В рамках выступления на Восточном экономическом форуме Е. Лихачёва аргументировала свою позицию тем, что алгоритмы обрабатывают преимущественно нерелевантные или недостоверные данные, характеризующиеся как «информационный мусор». Примечателен её тезис о хронологическом аспекте проблемы: по мнению директора, эффективность ИИ могла бы быть существенно выше в период 25-летней давности, когда интернет-пространство отличалось более высоким качеством контента. Таким образом, выявляется фундаментальная проблема, стоящая перед музеями: необходимость балансирования между технологическим прогрессом и сохранением аутентичности и точности культурного нарратива.

Государственный Эрмитаж: модель системной кибербезопасности. На фоне эскалации цифровых рисков, инициированной глобальной технологической

трансформацией, отечественные музейные институции демонстрируют прогрессирующую эволюцию в конструировании многоуровневой защитной архитектуры. Катализатором этого процесса выступил проект Государственного Эрмитажа, осуществленный в стратегическом партнерстве с Ассоциацией «Безопасность туризма» при методологическом курировании ИКОМ России [5]. Вовлеченность Международного совета музеев, чей профессиональный авторитет легитимизирует вырабатываемые стандарты, обеспечила репрезентативность разработанного методического комплекса. Функция организации заключалась в апробации и адаптации международных нормативов к локальным операционным реалиям, что позволило синтезировать универсальные принципы кибербезопасности со специализированными требованиями культурных институтов. Публикация, завершающая цикл из шести отраслевых стандартов, репрезентует трансформацию защитной парадигмы – от реактивного устранения инцидентов к проактивному моделированию целостной системы безопасности.

Технологический прогресс как источник киберугроз. Императив создания целевого руководства детерминирован диалектикой технологического прогресса в музейной сфере: экспоненциальное наращивание цифрового потенциала одновременно интенсифицирует киберугрозы. Логистика современных музейных процессов, включающая регулирование масштабных архивов оцифрованных артефактов, функционирование иммерсионных виртуальных ландшафтов и сложных экосистем, формирует гипертрофированную поверхность для потенциальных атак. В данном контексте доминирующими вызовами выступают таргетированные компрометации конфиденциальных массивов данных, несанкционированные интрузии в информационные контуры, криптографический шантаж операционных процессов и тотальная девальвация цифровых активов учреждения [2, с. 99-100].

Методологическое содержание руководства по кибербезопасности. Методологическая значимость представленного руководства определяется его междисциплинарной природой и практико-ориентированным подходом. Публикация осуществляет не просто каталогизацию актуальных киберугроз, но и предлагает многоуровневую систему противодействия, интегрирующую технологические решения, организационные регламенты и нормативно-правовые аспекты. Особый акцент сделан на разработке алгоритмов цифровой гигиены, оптимизации управления доступом и создании системы мониторинга инцидентов. Уникальность методике придает включение сравнительного анализа резонансных кейсов, в том числе атак на Британский музей и Лувр, что визуализирует транснациональный характер современных киберрисков.

Важнейшим аспектом проекта становится его потенциал для формирования глобальной культуры безопасности. Разработанные стандарты, транслируя через каналы ИКОМ, способствуют консолидации международного музейного сообщества. Создание унифицированного понятийного аппарата и тиражируемых протоколов безопасности позволяет нивелировать региональные различия в подходах к защите информации. Это создаёт основу для формирования распределенной системы кибербезопаности, где опыт противодействия инцидентам, полученный в одной юрисдикции, становится достоянием всего профессионального сообщества.

Стратегический ответ на вызовы цифровой эпохи. Инициатива Эрмитажа формирует стратегический ответ на вызовы цифровой эпохи, выходящий за национальные рамки. Публикация не только систематизирует лучшие практики, во и выполняет координирующую функцию, устанавливая отраслевой эталон защиты. Разработка такой гармонизированной методологии создает предпосылки для эффективного противостояния киберпреступности на глобальном уровне, обеспечивая устойчивость культурных институций как хранителей цивилизационного наследия в условиях перманентной цифровой трансформации.

Заключение. Проведенный анализ демонстрирует, что формирование эффективной системы информационной безопасности в музейной сфере приобретает характер стратегического императива. Российские музеи, как показывает кейс Эрмитажа, переходят от разрозненных защитных мер к выстраиванию целостной архитектуры кибербезопасности, основанной на проактивных методологиях и международных стандартах. Перспективное развитие данного направления неразрывно связано с укреплением международного сотрудничества. Противодействие транснациональной киберпреступности требует консолидации усилий на глобальном уровне – создания единых протоколов безопасности, обмена оперативной информацией об инцидентах и выработки согласованных правовых механизмов. Интеграция российского опыта в международную практику и адаптация лучших мировых наработок позволят сформировать устойчивую экосистему безопасности, обеспечивающую сохранность всемирного культурного наследия в цифровую эпоху [4, с. 258].

Список источников и литературы:

1. Абдуллова, А. К. Международная борьба с киберпреступностью // Тенденции развития науки и образования. – 2025. – № 117(4). – С. 8 – 10.

2. Бондарева, Д. А. Международные принципы и подходы к криминализации киберпреступности // Высокотехнологичное право: точка бифуркации: Материалы V Международной научно-практической конференции. В 3-х частях, Москва - Красноярск, 15 – 16 февраля 2024 года. Москва: Национальный исследовательский университет «Московский институт электронной техники». – 2024. – С. 94 – 101.

3. Британков, А. СМИ: системы безопасности Лувра использовали пароль «Louvre» [Электронный ресурс] // Hi-Tech Mail. 5 ноября 2025 г. URL: https://hi-tech.mail.ru/news/136855-smi-sistemy-bezopasnosti-luvra-ispolzovali-parol-louvre/ (дата обращения: 06.11.2025 г.)

4. Кубков, М. А. Международное сотрудничество в противодействии киберпреступности. Современные тенденции // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий: Сборник научных трудов Международной научно-практической конференции, Москва, 18 апреля 2024 года. – Москва: Московский университет МВД РФ им. В.Я. Кикотя. – 2024. – С. 255 – 258.

5. Музеи в цифровую эпоху: Эрмитаж выпустил пособие по информационной безопасности для музеев [Электронный ресурс] // Государственный Эрмитаж. 4 августа 2025 г. URL: https://www.hermitagemuseum.org/news/news_239_25?lng=ru% (дата обращения: 01.11.2025 г.)

6. Эксперт: ИИ пока не применим в музейной сфере [Электронный ресурс] // Редакция сайта ТАСС. 4 сентября 2024 г. URL: https://tass.ru/obschestvo/21767601 (дата обращения: 31.10.2025 г.)

Розалина Валерьевна Карапетова,
Преподаватель ГБПОУ Краснодарского края «Краснодарский педагогический колледж»,
E-mail: rozeline@mail.ru

Rozalina Valeryevna Karapetova,
Teacher at the Krasnodar Pedagogical College of the Krasnodar Region
E-mail: rozeline@mail.ru

СОХРАНЕНИЕ ИСТОРИЧЕСКОЙ ПАМЯТИ О ГЕНОЦИДЕ СОВЕТСКОГО НАРОДА НАЦИСТАМИ И ИХ ПОСОБНИКАМИ В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ НА ОККУПИРОВАННОЙ ТЕРРИТОРИИ НА ОСНОВЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

PRESERVATION OF THE HISTORICAL MEMORY OF THE GENOCIDE OF THE SOVIET PEOPLE BY THE NAZIS AND THEIR ACCOMPLISHERS DURING THE GREAT PATRIOTIC WAR IN THE OCCUPIED TERRITORY BASED ON THE CAPABILITIES OF ARTIFICIAL INTELLIGENCE

Аннотация. Доклад посвящен значимым событиям, связанным с празднованием 85-й годовщины победы в Великой Отечественной войне. Автор подчеркивает важную роль исторических уроков и необходимость сохранения памяти о подвигах предков. Особое внимание уделяется сочетанию традиционных методов образования с современными технологиями искусственного интеллекта (ИИ). Использование инновационных подходов, таких как создание интерактивных материалов и виртуальных экскурсий, рассматривается как способ сделать обучение более привлекательным и эффективным. Однако подчеркивается, что технологии не заменяют личное взаимодействие учителя и ученика, которое играет ключевую роль в воспитании молодого поколения.

Ключевые слова: Великая Отечественная война, историческая память, искусственный интеллект, образовательные технологии, патриотическое воспитание.

Abstract: The report focuses on significant events associated with the 85th anniversary of victory in the Great Patriotic War. The author emphasizes the important role of history lessons and the need to preserve the memory of our ancestors' exploits. Particular attention is paid to combining traditional educational methods with modern artificial intelligence (AI) technologies. The use of innovative approaches, such as the creation of interactive materials and virtual tours, is seen as a way to make learning more engaging and effective. However, it is emphasized that technology cannot replace personal interaction between teacher and student, which plays a key role in educating the younger generation.

Keywords: Great Patriotic War, historical memory, artificial intelligence, educational technologies, patriotic education.

В этом году наша страна отметила 85-летие со дня Победы в Великой Отечественной войне. Как сказал президент России В.В. Путин 9 мая 2025 года, «мы помним, что судьба человечества решалась в грандиозных битвах под Москвой и Ленинградом, Ржевом, Сталинградом, Курском и Харьковом, под Минском, Смоленском и Киевом, в тяжёлых кровопролитных боях от Мурманска до Кавказа и Крыма». «Россия сейчас переживает сложный, рубежный период. Судьба Родины, её будущее зависит от каждого из нас» [1].

Спустя месяц, на заседании Петербургского международного экономического форума президент отметил, что «Важно не только разрабатывать новые технологические решения, но и оперативно внедрять их в жизнь» [3].

В своей педагогической практике мы решили совместить сохранение исторической памяти и возможности технологий искусственного интеллекта. Этот шаг предоставляет огромные возможности, но вместе с тем ставит и серьезные вопросы, требующие взвешенного и обдуманного подхода. Сегодня мы постараемся рассмотреть эту тему, выявить потенциальные преимущества и риски, а также определить, как можно эффективно и этично интегрировать ИИ в образовательный процесс.

ИИ позволяет создавать новые образовательные инструменты, такие как интерактивные материалы, виртуальные экскурсии и обучающие видео. Эти инструменты делают обучение более увлекательным и интерактивным, что способствует лучшему усвоению материала. При этом ИИ не способен заменить человеческое общение и эмоциональную поддержку, которые так важны для развития личности. Учитель – это не просто источник знаний, а наставник, который вдохновляет, поддерживает и помогает ученику раскрыть свой потенциал. Технологии должны быть инструментом, который помогает нам достигать образовательных целей, а не самоцелью.

Нетрадиционная форма проведения занятия урок-суд является эффективной, поскольку сочетает в себе различные виды самостоятельной деятельности обучающихся. В ходе подготовки рассматриваются различные исторические документы и факты, которые необходимо исследовать и буквально «пропустить через себя», чтобы представить точку зрения и мотивы всех участников заседания. Формируется чувство патриотизма и умение работать в команде. В ходе работы над проектом обучающиеся активно исследовали

материалы сайта «Без срока давности», работали с архивными документами, информационными источниками и мемуарами.

Обратимся к видеоматериалам, демонстрирующим преступления нацистов против детства. Вот история юного скрипача Муси Пинкензона – одиннадцатилетнего скрипача из станицы Усть-Лабинскую Краснодарского края. (Рис. 1)

Рис. 1. Видеоматериалы

Перейдя по коду, можно узнать историю 11-летнего Гарика Стародубцева, уроженца станицы Динской, ставшего партизаном. В августе 1942 года он пробрался в совхоз «Агроном», где стояла наша оборона, и вступил в конную разведку, разведал, где стоит обоз, батарея, бензовозы немецких войск и убил немецкого солдата. За отважную разведку и образцовое выполнение обязанностей связного, Гарик Стародубцев награжден медалью – «За боевые заслуги». При помощи нейросети мы оживили фотографии военной кинохроники и озвучили бессмертные строки стихотворения А.Т. Твардовского «Рассказ танкиста», а также связали события Великой Отечественной войны и Специальной военной операции словами стихотворения Ксении Мальцевой «Ты вернешься домой, солдат». (Рис. 2)

Рис. 2. Видеоматериалы

На уроке ожила история Алексея Лебедева. Этому мальчику с большими и взрослыми глазами на снимке 12 лет. Он оказался среди тех, кто сумел выжить в Освенциме. Там ему и присвоили номер, который он показывает на фотографии. Номер 158671, который остался с ним на всю жизнь, как память о детстве, которого не было. Война забрала у него все, – отца, мать, сестер. Он вырос в Киевском детском доме, а когда вырос – закончил вуз и стал дипломатом. К сожалению, его не стало в 1972 году, когда ему было 38 лет. Все эти материалы были представлены на занятии в ходе заседания суда «Нюрнбергский процесс». Рис. 3

Рис. 3 Алексей Лебедев

Заключение. Сегодня важно подготовить высококвалифицированных будущих специалистов, воспринимающих судьбу Отечества как свою собственную. Без знания своего исторического прошлого нет будущего. Сегодняшние обучающиеся педагогического колледжа – это будущие педагоги и родители. От их слова и дела зависит наше «завтра». Если в течение года они будут узнавать страницы истории и делиться этим в доступной и современной форме со сверстниками, то в дальнейшем смогут передать свои знания следующим поколениям.

Список источников и литературы:

1. Путин В.В.: РФ должна отстаивать историческую правду о событиях Второй мировой [Электронный ресурс] // URL: www.gazeta.ru (дата обращения: 25.10.2025).

2. Путин: новая архитектура безопасности должна быть равной и неделимой [Электронный ресурс] // URL: tvzvezda.ru (дата обращения: 27.10.2025).

3. Путин с Красной площади обратился к россиянам. [Электронный ресурс] // URL: www.tvc.ru (дата обращения: 27.10.2025).

Алина Сергеевна Черненко,
Студентка 3 курса ГБПОУ Краснодарского края «Краснодарский педагогический колледж»,
E-mail: rozeline@mail.ru

Alina S. Chernenko,
Third-year student at the Krasnodar Pedagogical College, Krasnodar Krai
E-mail: rozeline@mail.ru

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ НА УРОКЕ ЛИТЕРАТУРНОГО ЧТЕНИЯ В НАЧАЛЬНЫХ КЛАССАХ

USING NEURAL NETWORKS IN LITERARY READING LESSONS IN PRIMARY SCHOOLS

Аннотация. Статья рассматривает внедрение ИИ в образовательный процесс начального литературного чтения на примере анализа и визуализации поэмы Н.А. Некрасова «Крестьянские дети». Используются инструменты нейросетей для генерации изображений и анимации, что облегчает восприятие и понимание детьми художественных произведений. Приведены пошаговые инструкции по созданию мультимедийных материалов, иллюстрирующих сцены из произведения. Такой подход не только стимулирует интерес к чтению, но и развивает креативность, мышление и способность воспринимать художественные образы.

Ключевые слова: литературное чтение, детская литература, искусство, графика, иллюстрация, ИИ, нейросеть, анимация.

Abstract. The article explores the integration of AI into the educational process of elementary literary reading, using the analysis and visualization of N.A. Nekrasov's poem "Peasant Children" as an example. Neural network tools are used to generate images and animations, facilitating children's perception and understanding of literary works. Step-by-step instructions for creating multimedia materials illustrating scenes from the work are provided. This approach not only stimulates interest in reading but also develops creativity, thinking, and the ability to perceive artistic images.

Key words: literary reading, children's literature, art, graphics, illustration, AI, neural network, animation.

Литературное чтение – один из важнейших предметов начальной школы. Именно здесь младшие школьники узнают буквы и учатся читать свои первые слова. Этот предмет

учит детей работать с текстом и пробуждает интерес к чтению художественной литературы, тренирует память, способствует общему развитию и духовно-нравственному воспитанию. Учащиеся имеют возможность сопереживать героям и оценивать их поступки, выражать свои чувства и эмоции, делать предположения и прогнозы развития событий.

Для того чтобы младшие школьники лучше усвоили материал учебной программы, учителю недостаточно его знать, необходимо уметь его преподнести так, чтобы ребятам захотелось читать и узнавать больше о героях. На педагогических факультетах и в колледжах существует предмет «Детская литература». Благодаря этой дисциплине будущих преподавателей учат работе с буквами, текстами и детскими произведениями.

Практически каждому ребёнку для лучшего понимания и запоминания той или иной информации необходима наглядность. Раньше она представляла собой рисунки и фотографии в детских книгах. Даже сейчас, если мы найдем на интернет-ресурсах сайты с детскими произведениями, то увидим рисунки несмотря на то, что произведения в онлайн формате. Это один из отличительных признаков детской литературы.

С ростом человеческих возможностей стали появляться фильмы и мультфильмы. Они точно так же знакомят младших школьников с произведениями детской литературы, но тут уже не акцентируется внимание на чтении, они сами рассказывают ребёнку историю. Всё, что требуется от него – заинтересованность в процессе просмотра. Конечно хорошо, если перед этим ученик ознакомлен с произведением, но зачастую этого даже не требуется. Фильмы и мультфильмы рассказывают полноценную историю с нуля.

На данном этапе человеческого развития искусственный интеллект (ИИ), он же нейросеть, оказывает всё более значительное влияние на образование детей и молодёжи. Он предоставляет абсолютное новые возможности для обучения, делает его более качественным и эффективным. С его помощью преподаватели могут кардинально поменять свой подход к обучению, внедряя нейросети в свои уроки. В данной статье мы рассмотрим несколько приложений ИИ и возможность его внедрения в общеобразовательную дисциплину начальной школы Литературное чтение на примере поэмы Николая Алексеевича Некрасова «Крестьянские дети». Попробуем самостоятельно сделать мультфильм.

Первый сайт для использования ИИ, который мы рассмотрим – Artguru. У этого сайта довольно много возможностей. Он может сделать фото более чётким, вырезать какой-либо объект, удалить фон и даже сгенерировать картинку и фотографию по вашему описанию, что нам и нужно. Для этого заходим на сайт в любом удобном Вам поисковике, в меню ищем иконку «Нейросеть рисует по описанию» и нажимаем. После этого перед нашими глазами появляется страница со строкой для ввода текста, в которую нам нужно

ввести описание необходимой фотографии. Будет лучше, если Вы введёте не строчку из произведения, а самостоятельно опишете фотографию. Так искусственному интеллекту будет проще её сгенерировать. Например, возьмём описание крестьянского мальчика у Николая Некрасова:

И, шествуя важно, в спокойствии чинном,
Лошадку ведет под уздцы мужичок
В больших сапогах, в полушубке овчинном,
В больших рукавицах… а сам с ноготок!

Если мы введём в строку запросов нейросети эти строки, ИИ, скорее всего, выдаст неточную или некрасивую картинку, поэтому нам стоит изменить запрос на более понятный. Просим искусственный интеллект нарисовать маленького мальчика в больших сапогах, полушубке и лошадкой рядом. Так ИИ выдаст более приемлемую картинку. (Рис. 1) Таким образом делаем каждую необходимую нам сцену.

Рис. 1. Крестьянский мальчик

Следующий сайт, который мы будем рассматривать – Runway. На данном сайте нам необходимо пройти регистрацию, после чего у нас появится несколько возможностей, одна из которых – «оживление» фотографии, создание из неё видео. Её мы и будем использовать. Всё, что нам нужно – загрузить уже имеющуюся фотографию, которую мы сгенерировали до этого, на сайт и описать действие, которое мы хотим получить на видео. Нажимаем кнопку сгенерировать – и готово. Нейросеть создаёт нам видео длиной в 10 секунд. Остаётся только соединить кусочки в одно видео в любом удобном вам приложении для монтажа, например, CapCut, и озвучить.

Наложить голос на видеоряд можно тоже с помощью ИИ. Для этого нам необходимо зайти на сайт FREENNS.RU и ввести нужный текст. На сайте есть возможность озвучки разными голосами, в зависимости от нужного Вам. Важно помнить, что нейросеть не может подобрать подходящую интонацию и не всегда ставит ударения в нужных местах, так же

ей тяжело даются стихи, из-за чего они могут звучать странно. Младшим школьникам может быть тяжело долго слушать такой голос, поэтому надо быть осторожным.

Процесс создания мультфильма не очень сложный, поэтому его можно практиковать в школе с учениками. Один из примеров урока – групповое создание мультипликационного видео. Для этого класс необходимо поделить на несколько групп, среди которых они разделят обязанности: создание картинок и фотографий, «оживление» фотографий, озвучка, монтаж видео. После создания мультфильма можно провести среди обучающихся класса конкурс, победители которого получат поощрение. Такая работа будет учить ребят взаимодействовать друг с другом, проявлять креативность, и лучше познакомит их с произведением, которое они изучают.

Заключение. Важно помнить, что использование искусственного интеллекта – это лишь помощь педагогу, а не полная его замена. Не стоит злоупотреблять нейростью в процессе обучения, но полное его игнорирование в современном мире всё больше становится невозможным.

Список источников и литературы:

1. Литературное чтение как учебная дисциплина. – [Электронный ресурс]. – Режим доступа: URL: https://spravochnick.ru/pedagogika/literaturnoe_chtenie_kak_uchebnaya_disciplina/ (дата обращения: 18.10.2025).

2. Нейросеть Artguru. – [Электронный ресурс]. – Режим доступа: URL: https://www.artguru.ai/ru/create/ (дата обращения: 21.10.2025).

3. Нейросеть Runway. – [Электронный ресурс]. – Режим доступа: URL: https://app.runwayml.com/login (дата обращения: 25.10.2025).

4. Нейросеть FREENNS.RU. – [Электронный ресурс]. – Режим доступа: URL: https://freetts.ru/ (дата обращения: 20.10.2025).

Александра Викторовна Волченкова,
ГБОУ г. Москвы «Школа № 1793 им. Героя Советского Союза А.К. Новикова», учитель,
РУДН имени Патриса Лумумбы, Факультет гуманитарных и социальных наук, магистрант 2 курса,
E-mail: volchenkova.a.v@lyc1793.ru

Aleksandra V. Volchenkova,
State school “School No. 1793 named after Hero of the Soviet Union A.K. Novikova", Peoples' Friendship University of Russia. P. Lumumbi,
E-mail: volchenkova.a.v@lyc1793.ru

КИБЕРБЕЗОПАСНОСТЬ СОВРЕМЕННОГО ШКОЛЬНИКА: КАК НЕ СТАТЬ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИЧЕСТВА?

CYBERSECURITY FOR SCHOOLCHILDREN TODAY: HOW NOT TO BECOME A VICTIM OF ONLINE FRAUD?

Аннотация. В эпоху цифровых технологий школьники проводят значительную часть времени онлайн. Виртуальное пространство предоставляет возможности для обучения, общения и развлечений, однако, повышает риск стать жертвой интернет-мошенничества. Недостаточная осведомленность и психологическая восприимчивость делают обучающихся уязвимыми перед злоумышленниками. Каждый год фиксируется большое количество случаев, когда школьники становятся жертвами фишинговых атак, мошенничества в социальных сетях, а также различных схем, связанных с онлайн-играми.

Ключевые слова: интернет, кибербезопасность, социальные сети, цифровые технологии.

Abstract. Today’s digital era sees schoolchildren spending much of their time online. While the Internet provides valuable opportunities for education, socializing, and leisure, it also exposes young users to the growing threat of online scams. Due to limited awareness and psychological vulnerability, students are particularly at risk. Every year, a large number of cases are recorded in which schoolchildren become victims of phishing attacks, fraud on social networks, as well as various schemes and connections with online games.

Key words: the Internet, cybersecurity, social media platforms, digital technologies.

Влияние возраста, опыта и онлайн-среды на уязвимость подростков к мошенничеству. Подростковый возраст, характеризуется интенсивностью когнитивного и социально-эмоционального развития. Обычный подросток представляет собой особую группу риска в отношении мошеннических схем. Уязвимость подростков к манипуляциям со стороны мошенников позволяет легко обмануть и подвергнуть опасности школьника.

Подростковый возраст характеризуется склонностью к рискованному поведению, повышенной импульсивностью и быстрому реагированию на ситуации. Всё это делает подростков более восприимчивыми к предложениям, поступающим со стороны мошенников о быстром и легком заработке или возможности испытать новые ощущения.

Недостаточный жизненный опыт школьника и недостаток знаний в области финансов и безопасности затрудняют оценку правдоподобности мошеннических предложений и понимание возможных последствий участия в незаконных действиях.

Каждый современный школьник пользуется различными социальными сетями и мессенджерами. Долгое пребывание в онлайн-среде характеризуется постоянной коммуникации со сверстниками, а также к контактам с субъектами, чья идентичность и социальная история остаются неизвестными для школьника. Иногда это подписки на проверенные источники, иногда – неизвестные корпорации и компании, сопряженные с нелегальной деятельностью или дезинформацией.

Анализ статистики преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, свидетельствует о возрастающей роли сети Интернет и, в частности, интернет-мессенджеров, в качестве инструментов для совершения противоправных действий. В контексте анализа динамики киберпреступности, по данным МВД России, отмечается тенденция к росту использования злоумышленниками возможностей сети Интернет. Согласно информации, опубликованной редакцией сайта ТАСС, наблюдается увеличение доли преступлений, совершенных с использованием Интернет каналов коммуникации: «При совершении ИКТ-преступлений на 2,2% возросло использование злоумышленниками сети Интернет (355 тыс. 182), на 35% - средств мгновенного обмена сообщениями (интернет-мессенджеры). Таких преступлений - 162 тыс. 318», - уточнили в министерстве [1].

При этом, несмотря на значительный рост использования методов социальной инженерии, количество преступлений и мошеннических схем, совершенных с помощью мессенджеров, превышает аналогичный показатель: «На 85% выросло использование методов социальной инженерии (таких преступлений 129 тыс. 006)», - сообщили в МВД [1]. Указанные данные приводятся в рамках общей статистики, согласно которой «всего в январе-июле 2025 года зарегистрировано 424,9 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» [1].

Мошеннические схемы обмана школьников в интернете. В сети Интернет существует целый ряд мошеннических схем, направленных на эксплуатацию несовершеннолетних пользователей. Самые распространенные схемы связаны с онлайн – играми, быстрым и

относительно простым способом заработать, ложными сообщениями о выигрышах, распространение вредоносного программного обеспечения и дроппинге. По данным компании «Мегафон», зафиксирован значительный рост случаев мошенничества, направленных на школьников, при этом злоумышленники все чаще представляются сотрудниками образовательных учреждений.

С начала 2025 года мошенники все чаще выдают себя за представителей школы: завучей, социальных педагогов. Схемы обмана могут быть различными, как и действия, которые должны выполнить школьники: в каких-то случаях ученикам предлагают зарегистрироваться на определенном ресурсе, в другом - назвать код из СМС для якобы активации школьного дневника, а иногда просят уточнить персональные данные родителей. За первые пять месяцев 2025 года таких инцидентов зарегистрировано на 30% больше, чем за весь прошлый год. [2]

Простые способы безопасности в сети Интернет. Так как дети все больше времени проводят в интернете, возрастает риск столкновения с мошенниками, которые используют различные тактики для обмана и кражи личных данных. Самое простое и важное правило интернет – безопасности школьника и любого интернет - пользователя это минимизация или полное исключение публикаций с использованием персональных данных:

- ФИО
- Паролей от личных кабинетов и аккаунтов
- ПИН-коды и CVV-коды банковских карт
- Фотографии паспортов, банковских карт и прочих документов, содержащих конфиденциальные сведения

Перед совершением финансовых операций, таких как оплата товаров, услуг или перевод денежных средств, убедитесь в безопасности сайта. Признаки безопасности включают:

- Использование протокола https:// в адресной строке
- Наличие значка замка в адресной строке [3]

Широкие возможности интернета сопряжены с рисками, поскольку даже,
казалось бы, незначительные публикации – компрометирующие фотографии, резкие высказывания или личная информация – могут оставить долгосрочный и не всегда желательный след в онлайн-пространстве. Важно понимать, что любая информация, размещенная в сети, мгновенно становится потенциально общедоступной. Важно понимать, что настройки приватности не гарантируют полной защиты, поскольку существует вероятность утечки данных или несанкционированного доступа к аккаунтам.

В цифровой среде многие современные приложения и веб-сайты оснащены функциями геолокации, которые позволяют определять и передавать данные о местоположении пользователя. Крайне важно осознавать потенциальные риски, связанные с демонстрацией своей геолокации и воздерживаться от автоматического согласия на подобные запросы в приложениях. Открытое раскрытие информации о местоположении может подвергнуть интернет - пользователя различным опасностям, начиная от преследования онлайн-мошенниками, способными установить их местонахождение, и заканчивая риском кражи личных данных.

Заключение. Уязвимость подростков в сфере кибербезопасности, обусловленная их недостаточной финансовой грамотностью, стремлением к самореализации и желанием быстрого заработка вызывает особую тревогу. Мошенники активно эксплуатируют эти особенности, используя различные схемы, такие как фишинговые сайты, объявления о легком заработке, онлайн-игры с элементами инвестиций, вредоносные программы и ложные сообщения о выигрышах. Для эффективной защиты подростков от интернет-мошенничества необходимо внедрение комплексных мер, включающих повышение осведомленности о киберугрозах, обучение правилам безопасного поведения в сети Интернет, развитие критического мышления и бдительности. Важным аспектом является активное участие родителей в контроле онлайн-активности детей и обучении их правилам кибербезопасности. Совместные усилия образовательных учреждений, родителей и правоохранительных органов позволят обеспечить надежную защиту подростков от кибермошенничества и возможность создать для них безопасное онлайн-пространство.

Список источников и литературы:

1. В России число мошенничеств с использованием мессенджеров выросло на треть. ТАСС, 1 сентября, 7:00. URL: https://tass.ru/obschestvo/24920281 (дата обращения: 11.11.2025).

2. Школьники все чаще становятся жертвами мошенничества. РИА НОВОСТИ, 2 июня, 03:13. URL: https://ria.ru/20250602/moshennichestvo-2020365090.html (дата обращения: 15.11.2025).

3. Открытый бюджет города Москвы. Распространенные виды мошенничества в сети интернет в отношении подростков. 7 марта 2024. URL: https://budget.mos.ru/fin-literacy/147 (дата обращения: (17.11.2025).

Дарья Эдуардовна Прокопчук,
Студент, ЧОУ ВО ЮУ (ИУБиП), г.Ростов-на-Дону
Email: prokopcukdara99@mail.ru

Daria E. Prokopchuk,
Student, Private Educational Institution of Higher Education "South Ural Institute of Management, Business, and Law", Rostov-on-Don
Email: prokopcukdara99@mail.ru

МОНИТОРИНГ ЦИФРОВОГО СОЗНАНИЯ СТУДЕНТОВ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА

MONITORING STUDENTS' DIGITAL CONSCIOUSNESS USING INTELLIGENCE ANALYSIS

Аннотация. Разработана архитектура системы мониторинга цифрового сознания студентов, основанная на агрегации данных из метавселенной, ИТ-лаборатории и чат-бота. Предложена методика расчета интегрального показателя через три суб-индекса. Описана аналитическая структура системы, генерирующей персональные рекомендации для самостоятельного развития студентов.

Ключевые слова. Цифровое сознание, образовательная аналитика, мониторинг учебной деятельности, метавселенная, персонализированные рекомендации.

Abstract. An architecture for a student digital consciousness monitoring system has been developed, based on the aggregation of data from the metaverse, IT lab, and chatbot. A method for calculating an integrated indicator using three sub-indices has been proposed. The analytical structure of the system, which generates personalized recommendations for student self-improvement, is described.

Key words. Digital consciousness, educational analytics, monitoring of educational activities, metaverse, personalized recommendations.

Введение. Современный образовательный процесс активно интегрирует цифровые среды, такие как метавселенные, чат-боты и проектные лаборатории. Однако данные, генерируемые в этих средах, часто остаются разрозненными и не используются для формирования целостной картины учебной деятельности [1, с. 45]. Это создает потребность в инструменте, который бы агрегировал и анализировал данную информацию, предоставляя студенту обратную связь для осознанного управления своей учебной траекторией [9, с. 80].

Целью работы является разработка модели и архитектуры системы мониторинга «цифрового сознания» – интегрального показателя, отражающего ключевые аспекты учебной деятельности студента в цифровой среде.

Концепция и метрики цифрового сознания. Под цифровым сознанием понимается комплексная характеристика, отражающая эффективность учебной деятельности студента в цифровой среде [3, с. 15]. Она формируется тремя компонентами:

1. Когнитивная глубина (КГ): способность к сложному анализу и решению нетривиальных задач [9, с. 82].
2. Социальная активность (СА): способность к коллаборации и совместной продуктивной работе [1, с. 48].
3. Цифровая инициативность (ЦИ): проактивность в освоении цифровых инструментов и сред [2, с. 25].

Для каждого компонента на основе данных из доступных источников разработан расчетный индекс.

Методика расчета индексов.

1. Индекс когнитивной глубины ($I_{КГ}$) Рассчитывается на основе данных чат-бота (сложность ответов) и метавселенной (сложность проектов).

Когнитивная глубина выражается как: 0,6*сложность ответов+0,4*сложность проектов

Сложность ответов рассчитывается по результатам взаимодействия с чат–ботом. Рассчитывается:

$$\frac{\sum_{i=1}^{n}(L_i \cdot C_i)}{n \cdot L_{max} * Cmax}$$

Формула 1. Сложность ответов

Где:

L_i - длина i-го ответа в символах.

C_i - коэффициент сложности вопроса (1 - простой, 2 - средний, 3 - сложный), присвоенный ботом.

L_{max} - максимальная длина ответа среди всех студентов (для нормализации)

$C_{max} = 3$

Сложность проектов оценивается по дипломам/бейджам, полученным в метавселенной за выполнение проектов[2,5]. Рассчитывается:

$$\frac{\sum_{j=1}^{m} Dj}{n \cdot D_{max}}$$

Формула 2. Сложность проектов

Где:

D_j - вес (сложность) j-го диплома (1 - базовый, 2 - продвинутый, 3 - экспертный).

$D_{max} = 3$.

2. Индекс социальной активности(I_{CA})

Формируется на основе данных IT-лаборатории и метавселенной

Социальная активность выражается как: 0,5*проектная активность+0,3*качество сотрудничества+0,2*экспертная помощь

Проектная активность = количество совмест. проектов / 3

Качество сотрудничества = норма завершенных проектов * 0,5 + доля завершенных * 0,5

Экспертная помощь = количество решенных проблем / 5

3. Индекс цифровой инициативности ($I_{ЦИ}$)

Рассчитывается наа основе данных IT-лаборатории

Выражается как: 0,6*масштаб проектов+0,4*темп работы

Масштаб проектов = (норма проектов*0,6) + (средняя сложность проектов*0,4)

Тем работы = (норма завершенных проектов*0,7)+(скорость завершения*0,3)

Интегральный индекс цифрового сознания ($I_{ЦС}$)

Общий показатель вычисляется как взвешенная сумма частных индексов:

$I_{ЦС}=\alpha*I_{КГ}+\beta*I_{CA}+\gamma*I_{ЦИ}$

где $\alpha + \beta + \gamma = 1$. Для сбалансированного профиля рекомендуются веса: $\alpha = 0.4, \beta = 0.3, \gamma = 0.3$ [3, с. 18]

Аналитическая архитектура системы. Система построена на многоуровневой архитектуре, обеспечивающей сбор и анализ данных из метавселенной, чат-бота и ИТ-лаборатории [1, с. 50]. Данные проходят через ETL-конвейер, сохраняются в аналитическом хранилище и обрабатываются в вычислительном ядре для расчета индексов. Модуль анализа динамики выявляет тенденции, а генератор рекомендаций создает персонализированные советы. Результаты визуализируются в дашборде студента, позволяя отслеживать прогресс и корректировать образовательную траекторию [9, с. 85].

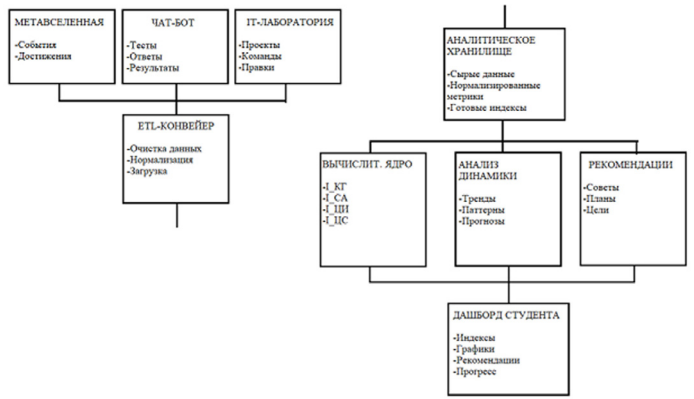


Рис.1. Аналитическая структура системы.

Заключение. Разработанная система открывает новые возможности для персонализации образования и развития самостоятельности студентов. Ее архитектура демонстрирует эффективный подход к преобразованию разнородных образовательных данных в практические рекомендации для саморазвития. Перспективы развития связаны с внедрением алгоритмов машинного обучения для прогнозирования успеваемости и проактивной поддержки студентов. Интеграция с дополнительными образовательными платформами позволит создать более полную картину учебной деятельности.

Дальнейшая работа будет направлена на разработку адаптивных алгоритмов, учитывающих индивидуальные особенности обучения, и создание мобильных приложений для обеспечения постоянного доступа к образовательной аналитике. В долгосрочной перспективе система может стать основой цифровых образовательных экосистем, где данные об учебной деятельности будут способствовать непрерывному совершенствованию образовательных программ и методик преподавания.

Список источников и литературы:

1. Андреев, А. А. Образовательная аналитика: методы и модели анализа цифрового следа студента / А. А. Андреев, Е. В. Лобанова // Высшее образование в России. – 2021. – Т. 30, № 5. – С. 45–58.

2. Бадаква, А. С. Формирование датасетов для искусственного интеллекта: основные проблемы и пути их решения / А. С. Бадаква, Б. В. Мартынов // Управление бизнесом и вызовы цифровой экономики : материалы V всероссийской (национальной) научно-практической конференции, Саратов, 14 февраля 2025 года. – Саратов: ООО "Амирит", 2025. – С. 5-12. – EDN MBKRHN.

3. Ковалева, Д. С. Цифровая трансформация образования: анализ данных и управление учебным процессом / Д. С. Ковалева, А. А. Федоров // Педагогическая информатика. – 2020. – № 3. – С. 15–27.

4. Мартынов, Б. В. Формирование правосознания как метод аттракции самоактуализационных форм деятельности / Б. В. Мартынов // Методология юридической науки: состояние проблемы, перспективы : сборник статей / отв. ред. М. Н. Марченко. – Москва : Юрист, 2008. – Вып. 2. – С. 41-49. – EDN VZZSRF.

5. Мартынов, Б. В. Самоактуализация человека: обновляющееся понимание в изменяющихся условиях : дис. … канд. филос. наук : 09.00.11 / Б. В. Мартынов. – Ростов-на-Дону, 2003. – 167 с. – EDN NMLXNH.

6. Смирнов, А. В. Цифровой след в образовании: методы анализа и интерпретации / А. В. Смирнов, И. А. Петрова // Образовательные технологии и общество. – 2022. – Т. 25, № 2. – С. 45–58.

7. Федоров, А. А. Метавселенные в образовании: возможности и вызовы / А. А. Федоров, Д. С. Ковалева // Высшее образование в России. – 2023. – Т. 32, № 1. – С. 112–125.

8. Иванова, Г. С. Метавселенные в профессиональном образовании: новые возможности и вызовы / Г. С. Иванова, К. Д. Петров // Образовательные технологии. – 2022. – № 4. – С. 23–35.

9. Яковлева, М. Н. Интеллектуальный анализ образовательных данных: методы и технологии / М. Н. Яковлева // Информатизация образования и науки. – 2021. – № 2(46). – С. 78–89.

Сергей Александрович Себекин,
К.и.н., старший научный сотрудник Факультета международных отношений Санкт-Петербургского государственного университета
E-mail: sebserg37@gmail.com

Sergey A. Sebekin,
Ph.D. in History, Senior Research Fellow, Faculty of International Relations, St. Petersburg State University
E-mail: sebserg37@gmail.com

СТРАТЕГИЧЕСКАЯ КОММУНИКАЦИЯ БРИКС В ЭПОХУ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ИНФОКРАТИИ: КАК ИНКЛЮЗИВНАЯ КОММУНИКАЦИЯ ЗАМЕНЯЕТСЯ СИНТЕТИЧЕСКИМ ИНФОРМАЦИОННЫМ ПОТОКОМ[12]

BRICS STRATEGIC COMMUNICATION IN THE ERA OF ARTIFICIAL INTELLIGENCE AND INFOCRACY: HOW INCLUSIVE COMMUNICATION IS BEING REPLACED BY SYNTHETIC INFORMATION FLOW

Аннотация. В работе рассматриваются перспективы осуществления стратегической коммуникации БРИКС в условиях инфократии. Анализируются угрозы, продуцируемые для осуществления стратегической коммуникации БРИКС со стороны режима инфократии в эпоху тотальной информатизации, сбора данных, информационного контроля и монополии цифровых платформ. Продемонстрировано, что инклюзивные информационные потоки заменяются алгоритмически предопределённым выбором, что несёт прямую угрозу открытой стратегической коммуникации и подрывает инклюзивные демократические процессы. Актуальность работы обусловлена фактической заменой инклюзивной коммуникации синтетическими информационными потоками, что ведет к потере государствами и объединениями контроля над коммуникационными каналами, и системному подрыву легитимности стратегических сообщений, тем самым ставя под угрозу достижение долгосрочных целей БРИКС.

Ключевые слова: стратегическая коммуникация, БРИКС, инфократия, информация, алгоритмическое правление, искусственный интеллект, цифровые платформы.

Abstract. This paper examines the prospects for BRICS strategic communication in an infocracy. It analyzes the threats posed to BRICS strategic communication by the infocracy regime

[12] *Исследование выполнено за счет гранта Российского научного фонда № 25-18-00699, https://rscf.ru/project/25-18-00699/*

in the era of total informatization, data collection, information control, and the monopoly of digital platforms. It demonstrates that inclusive information flows are being replaced by algorithmically predetermined choices, posing a direct threat to open strategic communication and undermining inclusive democratic processes. The relevance of this paper lies in the fact that inclusive communication is effectively being replaced by synthetic information flows, leading to states and associations losing control over communication channels and systemically undermining the legitimacy of strategic messages, thereby jeopardizing the achievement of BRICS' long-term goals.

Key words: strategic communication, BRICS, infocracy, information, algorithmic governance, artificial intelligence, digital platforms.

Сегодня БРИКС является динамично развивающимся объединением, претендующим на становление в качестве нового центра силы в мировой политике. Одним из эффективных инструментов достижения целей и построения нового миропорядка для БРИКС является стратегическая коммуникация (СК) – концепция, реализуемая государствами и объединениями с целью трансляции реально осуществляемых действий и дел.

В современном мире, в эпоху тотальной информатизации, сбора данных, информационного контроля и монополии цифровых платформ, когда инклюзивные демократические процессы и информационные потоки заменяются алгоритмически предопределённым выбором [6], СК БРИКС, нацеленная на становление объединения как нового центра силы и построение справедливого миропорядка, сталкивается с критическими вызовами инфократии – политико-социального режима, где власть сосредоточена в контроле над информационными потоками и цифровыми платформами.

В данном докладе будет рассмотрено, как инфократия и замена инклюзивных информационных потоков алгоритмическим выбором несёт прямую угрозу открытой стратегической коммуникации, и какие конкретные угрозы подрывают СК БРИКС.

Актуальность доклада обусловлена фактической заменой инклюзивной коммуникации алгоритмически предопределенным выбором, что ведет к потере государствами и объединениями контроля над коммуникационными каналами, и системному подрыву легитимности стратегических сообщений, тем самым ставя под угрозу достижение долгосрочных целей БРИКС.

Прежде чем перейти к рассмотрению и анализу угроз инфократии и алгоритмов для осуществления эффективной СК, необходимо создать концептуальную основу и определить ключевые понятия доклада.

Исходя из целей и задач доклада, мы определим СК БРИКС как системные, скоординированные и долгосрочные действия БРИКС и её стран-членов, направленные на создание устойчивого восприятия объединения как эффективной международной структуры, и осуществляемые посредством конкретных дел, многосторонней коммуникации с целевыми аудиториями, формированием дружественного БРИКС информационного пространства и трансляцией нужных стратегических сообщений для достижения конкретных целей БРИКС.

СК – инструмент реализации системного, долгосрочного и адекватного восприятия целевыми аудиториями реальных дел и действий БРИКС [1; 3; 4; 5].

Базовые инструменты СК – это конкретные действия и коммуникация.

Под делами и действиями субъекта СК можно понимать весь комплекс стратегических форм конкретной активности, осуществляемых в широком спектре общечеловеческой деятельности, и направленных на реализацию долгосрочных стратегических целей субъекта СК. Это может быть осуществление крупных проектов, международные инициативы, переговоры, планы действий и т.д.

Коммуникация – процесс трансляции стратегических сообщений на целевую область воздействия СК с целью формирования и закрепления определённых образов и нарративов у объекта СК.

СК – это не просто информационно-психологическое воздействие на целевые аудитории, а информационное продуцирование реальных действий. СК – «воздействие через действие» – реальные действия и их синхронизация с коммуникационным сопровождением (стратегическими сообщениями).

Важно выделить ряд ключевых характеристик СК.

I. Целенаправленность и преднамеренность – СК всегда направлена на достижение конкретных коммуникационных целей и на конкретную целевую аудиторию;

II. Мультинструментальность в достижении целей. СК подразумевает использование множества инструментов – сотрудничество, дипломатия, «мягкая сила», коммуникация и т.д.

III. Синхронизация – согласование реальных действий их информационное сопровождение посредством стратегических сообщений. и того, как это воспринимаются целевыми аудиториями

IV. Восприятие целевыми аудиториями субъекта СК, его действий и транслируемых стратегически сообщений.

V. Системность – СК подразумевает системный подход к реализации связанных и синхронизированных актов, сопровождаемых постоянным процессом коммуникации.

Таке важно выделить базовые для концепции СК понятия:

1. Стратегические сообщения СК – конкретные механизмы информационного воздействия, транслирующиеся посредством медиа-платформ, осуществляющиеся системно и направленные на формирование информационного пространства с целью достижения долгосрочных информационных стратегических целей субъекта СК.

2. Целевая область воздействия СК – целевая аудитория СК, территориальные рамки, и даже время и условия целевых обществ.

Если конкретные формы, инструменты и механизмы СК неэффективны, или наблюдается рассинхронизация между осуществляемыми действиями и посылаемыми стратегическими сообщениями, то СК может быть легко подавлена.

СК БРИКС формируется на основе демонстрации устойчивости объединения, эффективного сотрудничества, укрепления межнационального единства, унифицированной позиции по ключевым глобальным проблемам мирового развития и продвижения своих интересов на мировой арене. Важно, что СК БРИКС также подразумевает обязательную синхронизацию действий и стратегических сообщений.

Но что такое инфократия?

Инфократия – общественно-политическая и экономическая система, основанная на всеобъемлющем использовании цифровых технологий для достижения политико-экономических целей, при которой в качестве ключевых механизмов осуществления власти, управления и контроля над обществом и процессами используются цифровые технологии, информация и данные. Ключевой источник власти здесь – контроль над информацией и информационными потоками.

При инфократии власть сосредотачивается у тех субъектов, которые обладают монопольным доступом к технологиям и цифровым платформам, и, соответственно, сбору, анализу, распространению и стратегическому использованию информации для достижения политических, экономических и социальных целей – корпораций, государств, техно-элит. Между тем, можно наблюдать, что всё больше рычагов и механизмов осуществления власти сосредотачиваются именно у владельцев цифровых платформ и алгоритмов – транснациональных IT-корпораций – которые способны формировать информационное пространство и манипулировать информационными потоками. Они могут принимать решения о демонстрации того или иного контента, устанавливать и регламентировать правила публичных взаимодействий на платформах и допустимых нарративов, и настраивать функционал алгоритмов и цифровых платформ.

Для выявления и понимания вызовов и угроз, продуцируемых инфократией как общественно-технологической системы управления, необходимо рассмотреть основные признаки и инструменты её формирования.

Первый и ключевой признак инфократии – масштабный сбор данных о конкретных пользователях и огромных целевых аудиториях, и манипулирование самой информацией. Именно доступ к пользовательским данным и возможности их эксплуатации открывают механизмы по влиянию на массовое сознание, установлению и контролю над повесткой, настройки информационного пространства. Доступ к данным пользователей позволяет устанавливать совершенно новые уровни власти и открывает беспрецедентные возможности для конкретных механизмов контроля над пользователями. Так, в 2012 г. Facebook[13] провёл эксперимент по манипулированию новостной лентой 700 тыс. своих пользователей, удаляя либо все позитивные, либо все негативные посты, чтобы посмотреть, как это повлияет на их эмоциональное состояние [2].

Политика и экономическая логика при инфократии направлена на хищнический сбор и эксплуатацию пользовательских данных на цифровых платформах с целью их капитализации, манипуляции эмоциями пользователей для влияния на предпочтения и сознание с целью реализации коммерческих интересов и получения выгоды. При инфократии игнорируются интересы пользователей, а человек рассматривается с точки зрения логики полезности в качестве источника данных. При этом, такой сбор данных иногда не согласуется с нормами соблюдения конфиденциальности, этики и т.д.

Второй признак, вытекающий из первого – глобальное формирование алгоритмами информационного пространства, контроль над информацией и информационными потоками. При инфократии глобальное и национальное пространства формируются не естественным путем, а могут настраиваться заинтересованными акторами (корпорациями, владеющими цифровыми платформами и правительствами) для конкретных целевых аудиторий в целях информационного контроля над транслируемой повесткой.

Третий признак – «власть цифровых платформ», при котором цифровые социальные платформы выступают в качестве источника власти и предоставляют своим владельцам монопольное право не только на формирование информационного пространства и нарративов, но и позволяют контролировать даже социальные взаимодействия и общественную мобилизацию. Так, изменения механизмов работы любой социальной платформы (Facebook, YouTube), в том числе изменения в работе платформенных алгоритмов может изменить охват воздействия целевых аудиторий, глубже повлиять на

[13] Социальная сеть Facebook, принадлежащая Meta Platforms Inc., признана экстремистской и запрещена на территории РФ по решению Тверского районного суда г. Москвы от 21.03.2022.

формирование информационных нарративов, и, как следствие, на общественную мобилизацию.

При этом, ключевым инструментом формирования информационного пространства и контроля над нарративами выступают ИИ-алгоритмы. Информация при инфократии циркулирует не как нейтральный поток из разнообразных источников, а как отфильтрованный алгоритмами конкретный спектр таргетированных информационных нарративов. Таким образом, системы ИИ используются в качестве инструмента воздействия и масштабной настройки массового сознания.

Другой важнейший признак инфократии – алгоритмическое предопределение (политического) потребительского выбора. ИИ алгоритмы, интегрированы в современные социальные платформы, на основе анализа пользовательских предпочтений настраивают информационную ленту и демонстрируют таргетированный контент определённого содержания, релевантный для конкретного пользователя или целевой аудитории в результате чего пользователи помещаются в информационные эхо-камеры, в которых культивируется конкретная точка зрения, и игнорируются альтернативные информационные нарративы. В результате наблюдается алгоритмическая фрагментация целевых аудиторий и создание множества отдельных информационных сообществ, которые придерживаются собственных узких взглядов и игнорируют другие.

Итак, какие вызовы и риски алгоритмическая инфократия несёт для реализации стратегической коммуникации?

Во-первых, осуществление эффективной СК БРИКС и трансляция стратегических сообщений в условиях инфократии и монополий корпораций на владение социальными сетями, сбора данных и формирования глобального информационного пространства, становится труднодостижимой задачей силу того, что национальные государства и наднациональные объединения теряют контроль над информационными каналами. СК предполагает наличие инклюзивных информационных потоков, при которых субъект СК (БРИКС) способен эффективно транслировать свои стратегические цели, формировать стратегические сообщения и нарративы. В условиях алгоритмической инфократии это труднодостижимо, так как алгоритмы цифровых платформ массово настраивают контент и фильтруют стратегические сообщения через становление алгоритмических правил.

Во-вторых, происходит алгоритмическая социально-общественная фрагментация аудиторий. Эффективное осуществление СК предполагает наличие целостной и не фрагментированной аудитории, которая получает различные виды информации в равных объемах. При инфократии алгоритмы цифровых платформ помещают пользователей во множественные информационные эхо-камеры, формируя замкнутые фрагментированные

информационные сообщества. Это приводит к трудностям относительно трансляции единых стратегических сообщений, в результате чего нарративы могут дробиться и интерпретироваться целевыми аудиториями совершенно по-разному, что требует от субъекта СК таргетированной проактивной информационной стратегии.

В-третьих, при инфократии наблюдается асимметрия возможностей и ресурсов между национальными государствами и IT-корпорациями по формированию информационного пространства и трансляции нарративов в силу доступа этих негосударственных акторов к данным пользователей, монопольного владения цифровой инфраструктурой и способности устанавливать собственную политику модерации. Это в целом осложняет осуществление СК.

В-чётвертых, платформенные алгоритмы могут (даже непреднамеренно) подвергать стратегические сообщения субъекта СК модерации, деформировать и скрывать, подавлять их, и повышать в приоритете нарративы контрагентов. Динамика работы алгоритмов в рамках зарубежных цифровых платформ может сделать невозможным для субъекта СК долгосрочное удержание стратегических нарративов и сделать саму СК зависимой от работы алгоритмов.

В-пятых, в условиях инфократии СК БРИКС будет сталкиваться с угрозами высокотехнологичных информационно-психологических воздействий с применением ИИ – дипфейков, чат-ботов, которые будут осуществлять скоординированные сетевые операции и распространять подрывные стратегические сообщения.

Таким образом, главная угроза инфократии и алгоритмов для осуществления СК БРИКС состоит в том, что прямая, открытая и демократическая коммуникация, являющаяся основой непредвзятого выбора и инклюзивных демократических процессов (когда политика и решения разрабатываются путём относительно прямого диалога), в условиях инфократии по сути заменяется алгоритмически предопределённым выбором, при которым реальные решения замещаются иллюзией свободного демократического выбора [7].

Всё это может привести к реальной рассинхронизации стратегических сообщений и реальных действий субъекта СК и к системному снижению доверия со стороны целевых аудиторий к СК БРИКС, в результате чего коммуникация начинает восприниматься как манипуляция, а стратегические сообщения утрачивают легитимность.

В качестве механизмов противодействия, которые должны быть направлены на восстановление контроля над информационными потоками, коммуникацией и доверием, а также на адаптацию СК к условиям инфократии и алгоритмического управления, можно выделить:

1. Развитие национальных цифровых платформ и инфраструктуры в рамках БРИКС с целью снижения зависимости от транснациональных IT-корпораций с применением механизмов общественного и государственного контроля за новыми платформами. Развитие должно быть основано на принципах неотчуждаемого суверенитета.

2. Переход к многоканальной, таргетированной и проактивной стратегии реагирования, адаптирующей стратегические сообщения к фрагментированным информационным нишам для преодоления алгоритмической фрагментации.

3. Строгая синхронизация реальных действий и стратегических сообщений для восстановления доверия и предотвращения восприятия СК как манипуляции.

4. Использование технологий ИИ для мониторинга, верификации и быстрого реагирования на дипфейки и скоординированные сетевые кампании дезинформации.

5. Усиление системности СК, позволяющее удерживать долгосрочные нарративы.

Список источников и литературы:

1. Bazarkina, D. Y., Pashentsev, E. N. BRICS Strategic Communication: The Present and the Future // Russia in Global Affairs. 2021. Vol. 19, No. 3. P. 64-93

2. Hill, K. Facebook Manipulated 689,003 Users' Emotions For Science [Electronic resource] // Forbes. 2014. June 28. URL: https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/ (accessed: 27.03.2025).

3. Holtzhausen, D. R., Zerfass, A. The Routledge Handbook of Strategic Communication. London ; New York : Routledge, 2019.

4. Pashentsev, E. N. Strategic Communication in EU-Russia Relations // Strategic Communication in EU-Russia Relations: Tensions, Challenges and Opportunities / ed. E. N. Pashentsev. Cham : Palgrave Macmillan, 2020. P. 1-44.

5. Paul, C. Strategic Communication: Origins, Concepts, and Current Debates. Santa Barbara, CA : Praeger, 2011.

6. Ragacini, L. A., Santos, C. A. C. M. The infocracy: how digital flows disintegrate public discourse // Interference Journal. 2025. Vol. 11, No. 1. P. 312–330.

7. Williams, M. Social media democracy: How algorithms shape public discourse and marginalise voices // Journal of Media and Rights. 2025. Vol. 3, No. 1. P. 1-11.

Научное издание

III МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ КОНФЕРЕНЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник тезисов

Издано в авторской редакции

Компьютерная верстка: *И.О. Коваль*
Дизайн обложки: *В.Р. Хованская*

Подписано в печать 12.01.2026. Формат 60.90/16.
Гарнитура Minion Pro. Усл. печ. л. 14,75.
Тираж 500 экз. (1-й завод 30 экз.).
Издательство «РИТМ»
107176, г. Москва, ул. Стромынка, д. 18