БЮЛЛЕТЕНЬ

I МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

16 мая 2023 г.

Сборник тезисов

Москва

2023

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

Научный руководитель:
Яковенко Александр Владимирович,
Чрезвычайный и Полномочный Посол, член коллегии МИД России,
доктор юридических наук, профессор, ректор Дипломатической академии МИД России

Рецензенты:
Данельян Андрей Андреевич,
доктор юридических наук, профессор,
проректор по учебной работе и молодёжной политике
Дипломатической академии МИД России
Карпович Олег Геннадьевич,
доктор юридических наук, доктор политических наук, профессор,
проректор по научной работе Дипломатической академии МИД России
Крамаренко Александр Михайлович,
Чрезвычайный и Полномочный Посол,
директор Института актуальных международных проблем
Дипломатической академии МИД России

Ответственные редакторы:
Мартиросян Аревик Жораевна *– научный сотрудник Института актуальных международных проблем Дипломатической академии МИД России, член Совета молодых ученых Дипломатической академии МИД России, Российской Ассоциации международного права и Молодежного совета Координационного центра доменов.RU/.РФ*

Шангараев Руслан Насимович *– доктор политических наук, кандидат экономических наук, доцент, доцент кафедры стратегических коммуникаций и государственного управления Дипломатической академии МИД России, профессор Академии военных наук, главный редактор журнала «Вестник ученых-международников»*

Бюллетень I Международной молодежной конференции по информационной безопасности. Сборник тезисов / отв. ред. А.Ж. Мартиросян, Р.Н. Шангараев Дипломатическая академия МИД России. – М., 2023. – 270 с.

ISBN-978-5-6048376-1-0

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

Мнение авторов может не совпадать с мнением редакции. Редакция не несёт ответственности за высказанные авторами публикаций точки зрения на происходящие в России и в мире политические процессы, события, явления. При использовании материалов ссылка обязательна.

СОДЕРЖАНИЕ

ПРОГРАММА I МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6

ПОРЯДОК РАБОТЫ СЕКЦИЙ 8

ТЕЗИСЫ ДОКЛАДОВ УЧАСТНИКОВ I МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, 16 МАЯ 2023 Г. 18

СЕКЦИЯ 1. АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ТЕНДЕНЦИИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ 19

Басан Е.С., Рязанов М.С., Овсянникова В.А., Рядченко Т.Н., Шулика М.Г. Разработка сервиса для тестирования безопасности критической информационной инфраструктуры 20

Вдовкина Е.Д. Необходимость перехода к постквантовой криптографии . 33

Жбанов А.М. Ключевые факторы стратегического сдерживания в киберпространстве 36

Овчинников С.С., Овчинников В.С. Роль государственного служащего в обеспечении информационной безопасности 46

Терехова В.С. Деятельность Российской Федерации по обеспечению национальной информационной безопасности. 51

Тчанникова К.И. Информационное обеспечение безопасности космической инфраструктуры в контексте милитаризации 60

Цыплухин С.А. Использование информационно-коммуникационных технологий в военно-политических целях 68

Шао Цзысюань. Цифровая валюта как платежная революция в Китае – эффективная мера по продвижению борьбы с коррупцией и информационной безопасности. 71

СЕКЦИЯ 2. ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ 75

Ляшкевич М.В. Влияние использования инструментов международного политического маркетинга в социальных сетях на глобальную и региональную безопасность в контексте российско-украинского кризиса. 76

Серегина А.А. Информационно-психологическое воздействие в СМИ как угроза информационной безопасности РФ 80

Хаерова Э.М. Обнаружение поддельных новостей с использованием нейронных сетей LSTM 88

Чаморов Н.М. Использование социальных сетей и современных технологий в ходе ведения боевых действий 96

Чуклина Э.Ю. Противодействие распространению деструктивной информации в сети Интернет 102

СЕКЦИЯ 3. ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СОВРЕМЕННЫЕ МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ 111

Брачунова А.В. Конфликт в Южно-Китайском море как причина возникновения киберугроз в пространстве АСЕАН, Китая и США 112

Гаврилова А.С., Марков А.А. Информационная война как фактор угрозы для современной системы международных отношений 118

Иванов Е.О. Бразилия: эволюция подходов к информационной безопасности на пути к «цифровому суверенитету» 126

Клёстова В.А. Цифровые платформы в международных отношениях 135

Мищишина Е.В. Цифровизация международных отношений: угрозы и риски для Японии 144

Пичугин Н.В. Глобальные вызовы и угрозы в сфере информационной безопасности для КНР 158

Фроловская В.Д. Анализ вызовов и угроз в обеспечении информационной безопасности при использовании ИКТ в государственном управлении: сравнительный анализ Японии и России 164

Чернобривченко А.О. Международное сотрудничество в сфере защиты персональных данных: вызовы и угрозы 172

СЕКЦИЯ 4. МЕЖДУНАРОДНО-ПРАВОВОЕ ИЗМЕРЕНИЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ 183

Васильева А.А. Международно-правовые механизмы противодействия насилию над детьми в киберпространстве 184

Жебриков В.В. Проблемы квалификации международного преступления агрессии как акта, совершающегося в информационно-коммуникационном пространстве 189

Мамкин В.Ю. О международном компоненте обеспечения информационной безопасности при использовании интеллектуальных систем – вопросы и задачи правового регулирования 196

Савельева Н.В. Правовое регулирование спутниковой связи для обеспечения технологического суверенитета России 206

Трофимова О.С. Сравнительный анализ Стратегий национальной безопасности Российской Федерации и Соединенных Штатов Америки. 216

СЕКЦИЯ 5. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ..... 220

Воеводина И.А. Искусственный интеллект и информационная безопасность 221

Жеребятьев Д.Е., Калюжный Д.С. Аспекты применения машинного обучения для предотвращения кибератак 225

Забелич С.С. Использование искусственного интеллекта в процессе принятия внешнеполитических решений 232

Поднебесная Ю.Б. Особенности использования искусственного интеллекта в Израиле 242

Романов Р.Р. Искусственный интеллект в работе экспертно-аналитических центров: пример прогнозирования 249

Тимофеева А. Использование искусственного интеллекта в технологиях создания «дипфейков» как угроза информационной безопасности 252

Трофимова О.С. Морально-этический аспект искусственного интеллекта 258

Чичерина К.С. Методы машинного обучения и анализа данных в системе обнаружения фишинга и спама 264

ПРОГРАММА

I МЕЖДУНАРОДНАЯ МОЛОДЕЖНАЯ КОНФЕРЕНЦИЯ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

09:00 – 09:15

Ауд.4

ОТКРЫТИЕ КОНФЕРЕНЦИИ

Приветственное слово организаторов конференции

09:15 – 11:35

Ауд.4

Секция 1

«Актуальные проблемы и тенденции в сфере использования информационно-коммуникационных технологий»

11:35 – 12:45

Ауд.4

Секция 2

«Информационно-коммуникационные технологии и средства массовой информации»

13:30 – 16:00

Ауд.4

Секция 3

«Информационно-коммуникационные технологии и современные международные отношения»

16:10 –17:10

Ауд.4

Секция 4

«Международно-правовое измерение использования информационно-коммуникационных технологий»

17:20 – 19:10

Ауд.4

Секция 5

«Искусственный интеллект
и информационная безопасность»

17:00 – 18:00

Ауд. 6

Секция 6
Круглый стол по теме «Управление Интернетом»
организован совместно с Координационным центром доменов .RU/.РФ

ПОРЯДОК РАБОТЫ СЕКЦИЙ

Аудитория 4

09:15 – 11:35

Секция 1
«Актуальные проблемы и тенденции в сфере использования информационно-коммуникационных технологий»

Модераторы секции:

Мартиросян А.Ж. Научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

Степовая Д.А. Руководитель Департамента научной деятельности Школы МИБ, аспирант Московского государственного университета имени М.В. Ломоносова.

1. Ахмедов Э.Ю. К вопросу о кибертерроризме как угрозе национальной безопасности. Академия государственного управления при Президенте Республики Таджикистан.

2. Басан Е.С., Рязанов М.С., Овсянникова В.А., Рядченко Т.Н., Шулика М.Г. Разработка сервиса для тестирования безопасности критической информационной инфраструктуры. Институт компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета.

3. Вдовкина Е.Д. Необходимость перехода к постквантовой криптографии. Московский государственный технический университет имени Н.Э. Баумана.

4. Жбанов А.М. Ключевые факторы стратегического сдерживания в киберпространстве. Московский государственный университет имени М.В. Ломоносова.

5. Кашин Е.А., Крайнов С.К. Применение технологий информационных войн в 2020 году в Болгарии. Московский государственный университет имени М.В. Ломоносова.

6. Кострубова Д.Р. Защита государственного суверенитета в новом информационном пространстве. Государственный академический университет гуманитарных наук.

7. Мартынюк Э.Г. Актуальные проблемы цифрового терроризма и экстремизма. Московская академия Следственного комитета Российской Федерации.

8. Овчинников С.С., Овчинников В.С. Роль государственного служащего в обеспечении информационной безопасности. Московский государственный университет имени М.В. Ломоносова, Дипломатическая академия МИД России.

9. Озарнов Р.В. Особенности цифрового искусства как инвестиционного актива. Финансовый университет при Правительстве Российской Федерации.

10. Ржевская Н.В. Исследование угроз международной информационной безопасности. Северо-Кавказский федеральный университет.

11. Терехова В.С. Деятельность Российской Федерации по обеспечению национальной информационной безопасности. Тюменский государственный университет.

12. Тчанникова К.И. Информационное обеспечение безопасности космической инфраструктуры в контексте милитаризации. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

13. Цыплухин С.А. Использование информационно-коммуникационных технологий (ИКТ) в военно-политических целях. Российский государственный гуманитарный университет.

14. Чумаков В.А. Информация и дезинформация в современной дипломатии. Российский государственный университет имени А.Н. Косыгина.

15. Шао Цзысюань. Цифровая валюта как платежная революция в Китае — эффективная мера по продвижению борьбы с коррупцией и информационной безопасности. Московский государственный университет имени М.В. Ломоносова.

Аудитория 4

11:35 – 12:45

Секция 2
«Информационно-коммуникационные технологии и средства массовой информации»

Модераторы секции:

Зогранян Е.В. Аспирант Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

Мартиросян А.Ж. Научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

Степовая Д.А. Руководитель Департамента научной деятельности Школы МИБ, аспирант Московского государственного университета имени М.В. Ломоносова.

1. Каюрина Н.О. Цензура в социальных сетях КНР. Уральский федеральный университет имени первого Президента России Б.Н. Ельцина.

2. Ляшкевич М.В. Влияние использования инструментов международного политического маркетинга в социальных сетях на глобальную и региональную безопасность в контексте российско-украинского кризиса. Санкт-Петербургский государственный университет.

3. Серегина А.А. Информационно-психологическое воздействие в СМИ как угроза информационной безопасности РФ. Российско-Армянский государственный университет.

4. Стрелец А.В. Угрозы безопасности сетевых информационных систем. Финансовый университет при Правительстве Российской Федерации.

5. Хаерова Э.М. Обнаружение поддельных новостей с использованием нейронных сетей LSTM. Казанский национальный исследовательский технический университет имени А. Н. Туполева – Каи.

6. Чаморов Н.М. Использование социальных сетей и современных технологий в ходе ведения боевых действий. Донецкий государственный университет.

7. Чуклина Э.Ю. Противодействие распространению деструктивной информации в сети «Интернет». Южный научный центр Российской академии наук.

Аудитория 4

13:30 – 16:00

Секция 3
«Информационно-коммуникационные технологии и современные международные отношения»

Модераторы секции:

Мартиросян А.Ж. Научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

Степовая Д.А. Руководитель Департамента научной деятельности Школы МИБ, аспирант Московского государственного университета имени М.В. Ломоносова.

1. Булва В.И. Дипломатия в области международной информационной безопасности: перспективы «Кибергенассамблеи ООН». Московский государственный институт международных отношений (Университет) МИД России.

2. Брачунова А.В. Конфликт в Южно-Китайском море как причина возникновения киберугроз в пространстве АСЕАН, Китая и США. Самарский национальный исследовательский университет имени академика С.П. Королева.

3. Гаврилова А.С., Марков А.А. Информационная война как фактор угрозы для современной системы международных отношений. Санкт-Петербургский государственный экономический университет.

4. Иванов Е.О. Бразилия: эволюция подходов к информационной безопасности на пути к «цифровому суверенитету». Телеканал RT (испанская редакция).

5. Клёстова В.А. Цифровые платформы в международных отношениях. Санкт-Петербургский государственный университет.

6. Крылов Д.С. Идейно-ценностное воздействие Турции на процессы в информационном пространстве Республики Крым. Институт научной информации по общественным наукам Российской академии наук.

7. Мищишина Е.В. Цифровизация международных отношений: угрозы и риски для Японии. Московский государственный университет имени М.В. Ломоносова.

8. Перевозчикова К.С. Тенденции переходов конфликтов в информационное пространство как результат меняющегося мирового порядка. Крымский федеральный университет имени В.И. Вернадского.

9. Пичугин Н.В. Глобальные вызовы и угрозы в сфере информационной безопасности для КНР Институт статистических исследований и экономики знаний Высшей школы экономики.

10. Прончев К.Г. Глобальная цифровизация как фактор рационализации. Московский государственный университет имени М.В. Ломоносова.

11. Рохас Сампер Матео. Цифровая дипломатия в Латинской Америке. НИУ Высшая школа экономики.

12. Сбитнева А.И. Информационное влияние Турции на тюркоязычные народы России. Институт научной информации по общественным наукам Российской академии наук.

13. Фищук Н.В. Основы российской государственной политики в сфере международной информационной безопасности. Московский городской университет управления Правительства Москвы имени Ю.М. Лужкова.

14. Фроловская В.Д. Анализ вызовов и угроз в обеспечении информационной безопасности при использовании ИКТ в государственном управлении: сравнительный анализ Японии и России. Санкт-Петербургский государственный университет.

15. Чебыкина В.А. Роль тандема «Франция-ФРГ» в выстраивании системы диджитализации безопасности для нового мирового экономического цикла в XXI веке. Санкт-Петербургский государственный университет.

16. Чернобривченко А.О. Международное сотрудничество в сфере защиты персональных данных: вызовы и угрозы. Дипломатическая академия МИД России.

17. Шемякина Я.В. Обеспечение информационной безопасности: международное измерение. Член КСОРС Турции, Вице-президент по инновациям в России, АТИК.

Аудитория 4

16:10 –17:10
Секция 4
«Международно-правовое измерение использования информационно-коммуникационных технологий»

Модераторы секции:

Мартиросян А.Ж. Научный сотрудник ИАМП ДА МИД России, руководитель Школы МИБ.

Степовая Д.А. Руководитель Департамента научной деятельности Школы МИБ, аспирант Московского государственного университета имени М.В. Ломоносова.

1. Васильева А.А. Международно-правовые механизмы противодействия насилию над детьми в киберпространстве. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

2. Жебриков.В.В. Проблемы квалификации международного преступления агрессии как акта, совершающегося в информационно-коммуникационном пространстве. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

3. Мамкин В.Ю. О международном компоненте обеспечения информационной безопасности при использовании интеллектуальных систем – вопросы и задачи правового регулирования. Московский государственный юридический университет имени О.Е. Кутафина

4. Мельник С.С., Шестак В.А. Правовое регулирование киберэкстремизма и кибертерроризма: проблемы и перспективы. Московский государственный институт международных отношений (Университет) МИД России.

5. Савельева Н.В. Правовое регулирование спутниковой связи для обеспечения технологического суверенитета России. Московский государственный юридический университет имени О.Е. Кутафина

6. Трофимова О.С. Сравнительный анализ Стратегий национальной безопасности Российской Федерации и Соединенных Штатов Америки. Национальный центр управления обороной Российской Федерации.

Аудитория 4

17:20 – 19:10

Секция 5
«Искусственный интеллект и информационная безопасность»

Модераторы секции:

Зогранян Е.В. Аспирант Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

Третьяков А.Д. Аспирант Московского государственного университета имени М.В. Ломоносова.

1. Воеводина И.А. Искусственный интеллект и информационная безопасность. КПА Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

2. Голубева Т.Э. Искусственный интеллект и информационная безопасность. Дипломатическая академия МИД России.

3. Жеребятьев Д.Е., Калюжный Д.С. Аспекты применения машинного обучения для предотвращения кибератак. Кубанский государственный технологический университет.

4. Забелич С.С. Использование искусственного интеллекта в процессе принятия внешнеполитических решений. Российский государственный гуманитарный университет.

5. Зогранян Е.В. Искусственный интеллект как вспомогательный инструмент массового информационно-психологического воздействия. Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

6. Карасев П.А. Искусственный интеллект как фактор деградации стратегической стабильности. Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук.

7. Поднебесная Ю.Б. Особенности использования искусственного интеллекта в Израиле. Московский государственный университет имени М.В. Ломоносова.

8. Романов Р.Р. Искусственный интеллект в работе экспертно-аналитических центров: пример прогнозирования. Российский государственный гуманитарный университет.

9. Степанов В.А. Разработка алгоритма системы обнаружения атак, реализуемых с использованием методов социальной инженерии через сообщения электронной почты, а также экспериментальные исследования алгоритмов машинного обучения, выбранных перспективными. Национальный исследовательский университет ИТМО.

10. Тимофеева А. Использование искусственного интеллекта в технологиях создания «дипфейков» как угроза информационной безопасности. ФГБУ «НИИ «Интеграл»

11. Третьяков А.Д. Международная политика США в области использования искусственного интеллекта в военной сфере. Московский государственный университет имени М.В. Ломоносова.

12. Трофимова О.С. Морально-этический аспект искусственного интеллекта. Национальный центр управления обороной Российской Федерации.

13. Чичерина К.С. Методы машинного обучения и анализа данных в системе обнаружения фишинга и спама. Институт компьютерных технологий и информационной безопасности Южного федерального университета.

Аудитория 6

17:00 – 18:00

Секция 6
Круглый стол по теме «Управление Интернетом»
организован совместно
с Координационным центром доменов .RU/.РФ

Модератор секции:

Алейников А.А., председатель Молодёжного совета Координационного центра доменов .RU/.РФ.

1. Алейников А.А. Российские молодежные инициативы в области управления Интернетом. Молодёжный совет Координационного центра доменов .RU/.РФ.
2. Кулагина М.В. Российский подход к управлению Интернетом: история и перспективы. Дипломатическая академия МИД России.
3. Трусов С.А. Подготовка экспертов для представления интересов страны в международных организациях в отрасли ИКТ. Общественно-государственное объединение «Ассоциация документальной электросвязи».
4. Филина Н.А. Возможности участия молодежи в глобальных организациях и мероприятиях по управлению Интернетом. EURALO.
5. Хапов А.В. Молодёжь в ИТ: итоги Молодежного форума по управлению интернетом 2023. АНО «Центр компетенций по глобальной ИТ-кооперации»
6. Чалышева Ю.В. О деятельности Молодёжного цифрового омбудсмена. Член команды Молодёжного цифрового омбудсмена.

ТЕЗИСЫ ДОКЛАДОВ УЧАСТНИКОВ

I МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

16 МАЯ 2023 Г.

СЕКЦИЯ 1

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ТЕНДЕНЦИИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ»

Елена Сергеевна Басан
к.т.н., доцент каф. БИТ ИКТИБ ЮФУ
E-mail: ebasan@sfedu.ru

Максим Сергеевич Рязанов
студент каф. БИТ ИКТИБ ЮФУ
E-mail: riazanov@sfedu.ru

Виктория Александровна Овсянникова
студент каф. БИТ ИКТИБ ЮФУ
E-mail: ovsia@sfedu.ru

Татьяна Николаевна Рядченко
студент каф. БИТ ИКТИБ ЮФУ
E-mail: tivannikova@sfedu.ru

Мария Геннадьевна Шулика
ассистент каф. БИТ ИКТИБ ЮФУ
E-mail: mshulika@sfedu.ru

РАЗРАБОТКА СЕРВИСА ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. *На сегодняшний день разработка программных продуктов анализа безопасности является актуальной задачей, что обуславливается несколькими причинами. Во-первых, многие решения требуют дополнительных вычислительных мощностей при работе и могут значительно нагружать систему. Во-вторых, большинство из существующих решений достаточно сложны в настройке и требуют дополнительных знаний от специалиста, который осуществляет проверку.*

В данном исследовании был разработан прототип сервиса автоматизированного сбора данных о системе и верификации векторов атак исходя из собранных данных. Данный сервис предназначен для упрощения процесса сбора информации о системе для пользователей, а также проверки ее на предмет безопасности.

Ключевые слова: *кибербезопасность, критическая информационная инфраструктура, тестирование, кибератака, сервис, киберфизическая система.*

Обзор работ. Киберфизические атаки – это особая категория атак, которые негативно влияют на физическое пространство нацеливаясь на вычислительную и коммуникационную инфраструктуру, позволяющую людям и системам контролировать датчики и исполнительные механизмы [1].

В последние годы увеличилось количество кибератак, направленных на киберфизические системы (КФС), последствия которых достаточно разрушительны. Согласно текущим исследованиям, проведенным [2, 3], КФС очень подвержены атакам с внедрением вредоносного кода и атакам с повторным использованием кода, а также атакам с внедрением поддельных данных, данными с нулевым контролем и, наконец, атакам Control-Flow Attestation. Такие атаки могут привести к полному отключению промышленных устройств и КФС.

Прослеживаемость – инженерная концепция, которая позволяет удостовериться, что система во всей ее полноте, включая документацию и тестовые случаи, соответствует изменениям, внесенным на различных этапах разработки. В процессе разработки продукта и по мере возрастания сложности системы модели прослеживаемости не совершенствуются, не формализуются и не обновляются. В результате чего возникает несогласованность, проблемы с техническим обслуживанием и безопасностью, растет количество возможных кибератак. Формальные методы обеспечения прослеживаемости – очевидное решение, но их применение может привести к задержке выпуска продукта на рынок, что характеризуется высокими затратами [10]. Опыт работы с критичными к безопасности КФС, показывает, что систематическое применение формальных методов – редкость по причине отсутствия готовых методик, квалификации специалистов, времени и необходимых инструментов. Для устранения этого пробела нужны более простые методы.

В работах по безопасности КФС основное внимание уделяется тестированию на основе моделей, тестированию на основе поиска, онлайн-тестированию на основе мониторинга, тестирование на основе внедрения ошибок, тестирование на основе больших данных, облачное тестирование и особенно нефункциональное тестирование безопасности, на соответствие и прочность. Каким атакам подвержены КФС представлено в таблице 1.

Таблица 1 – Кибератаки

Тип уязвимости	**Тип киберугрозы**	**Атаки**
Сеть	- сетевой уровень, - уровень приложений, - физический уровень	Прослушивание, мошеннический узел, повторная атака; глушение связи, SYN-Flood, программы вымогатели; DOS/DDOS [4]
Платформа	- сетевой уровень, - уровень приложений, - физический уровень	Межсайтовый скриптинг, внедрение SQL, вредоносная 3-я сторона, ввод ложных данных, вредоносное ПО, бэкдор [5]
Управление	- сетевой уровень, - уровень приложений, - физический уровень	Взлом паролей, фишинг [6]

Многие испытательные стенды КФС сосредоточены на таких формах безопасности, как кибербезопасность, безопасность связи и физическая безопасность системы, информационная безопасность системы. Для интеллектуальных сетей разработано множество тестовых стендов [7, 8], ориентированных на кибербезопасность, которые можно использовать для проверки воздействия кибератак на интеллектуальные сети. Среди таких кибератак выделяют атаки типа отказ в обслуживании и атаки человек посередине путем моделирования и моделирования энергосистемы с помощью RTDS и RSCAD (программное обеспечение для моделирования RTDS). Network Simulator-3 (NS-3) и DeterLab могут использоваться для

моделирования сети связи, а также для «Мониторинга и управления стабильностью напряжения в реальном времени». Рассмотрим, какими инструментами тестирования обычно пользуются при оценке безопасности КФС в таблице 2.

Таблица 2 – Инструменты тестирования КФС

Инструменты	**Источники**	**Название**	**Описание**
Мю-8000	[9]	Mu Studio Security, построенная на мощной платформе автоматизации, которая обеспечивает обширную автоматизацию, отслеживает аппаратные и программные средства перезапуска и возможности создания отчетов	Интегрированная онлайн-документация состоит из четырех типов тестов, тестов на мутацию протоколов, включая промышленные протоколы DNP3, IEC 61850, MMS и MODBUS/TCP, генерирует пакеты тестов, содержащие мутации протоколов, безопасные цели успешно их обрабатывают, незащищенные цели могут реагировать ненормально
Cho	[10]	Инструмент Smart Fuzzing, который выполняет фаззинг на основе генерации и мутации	Требует создания файлов PeachPit для определения структуры и типа информации в данных, подлежащих фаззингу, позволяет настроить запуск фаззинга, включая передачу данных и ведение журнала интерфейса
Салли	[11]	Фреймворк для разработки и тестирования фаззеров	Он состоит из нескольких расширяемых компонентов, а также поддерживает модули фаззинга ICCP, modbus и DNP3
ШИП	[12]	Разработан, чтобы сосредоточиться на поиске эксплуатируемых ошибок	Это набор для создания фаззера, он предоставляет API, позволяющий пользователям создавать свои собственные фаззеры для сетевых протоколов, позволяет использовать язык программирования C

Алгоритм работы программного модуля. Архитектура программного модуля представляет собой совокупность двух сервисов: сервис сбора данных о системе и сервис проведения атак. Модуль сбора данных собирает необходимую информации об операционной системе *nix и локальной сети и сохраняет в файл расширением json. Модуль проведения атак принимает на вход файл сбора данных и на основании этих данных проводит атаки и верифицирует их. Данный процесс происходит в автоматическом режиме, пользователю нужно только запустить скрипт модуля сбора данных. Затем, когда модуль сбора данных отрабатывает, он отправляет данные на сервер, где развернут веб-интерфейс для подключения пользователя и удобства дальнейшего анализа. После обработки данных пользователь может определить, какие типы проверок он будет выполнять на в своей системе. Архитектура программного модуля представлена на рисунке 1.

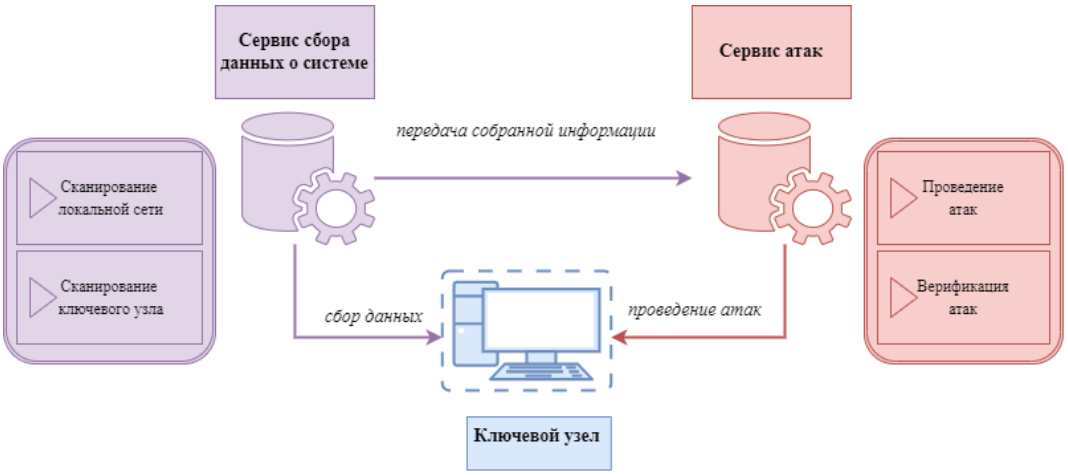


Рисунок 1 – Архитектура программного модуля

Сервис сбора данных о системе. Данный сервис собирает необходимую информацию о системе с помощью разработанного программного модуля. Программный модуль в автоматическом режимы собирает данные о системе путем выполнения наборов команд и возвращает их результат. Результат преобразовывается в читабельный для пользователя вид и сохраняется в файл. Программа собирает следующую информацию:

- IP-адрес хостовой машины,
- имя хостовой машины,

- наличие доступных сетевых интерфейсов хостовой машины и соответствующие им IP-адреса,

- текущий сетевой интерфейс,

- дистрибутив, его версия и описание,

- ядро Linux,

- MAC-адрес хостовой машины,

- работающие сервисы и их статус,

- установленные пакеты и их версия,

- системная информация о хостовой машине (модель устройства, информация о процессоре, оперативной памяти, внешние накопители, звуковая карта, сетевая карта, графическая видеокарта, USB-порты, подключенные устройства ввода/вывода, примонтированные к системе диски),

- TCP-порты локальной сети (номер порта, статус порта, информация о сервисе, на котором работает порт),

- UDP-порты локальной сети (номер порта, статус порта, информация о сервисе, на котором работает порт),

- IP-порты локальной сети (номер порта, статус порта, информация о сервисе, на котором работает порт),

- список установленных приложений (наименование, версия и описание).

На рисунке 2 представлен результат работы скрипта. Данный файл в таком формате далее отсылается на сервер для дальнейшего анализа.

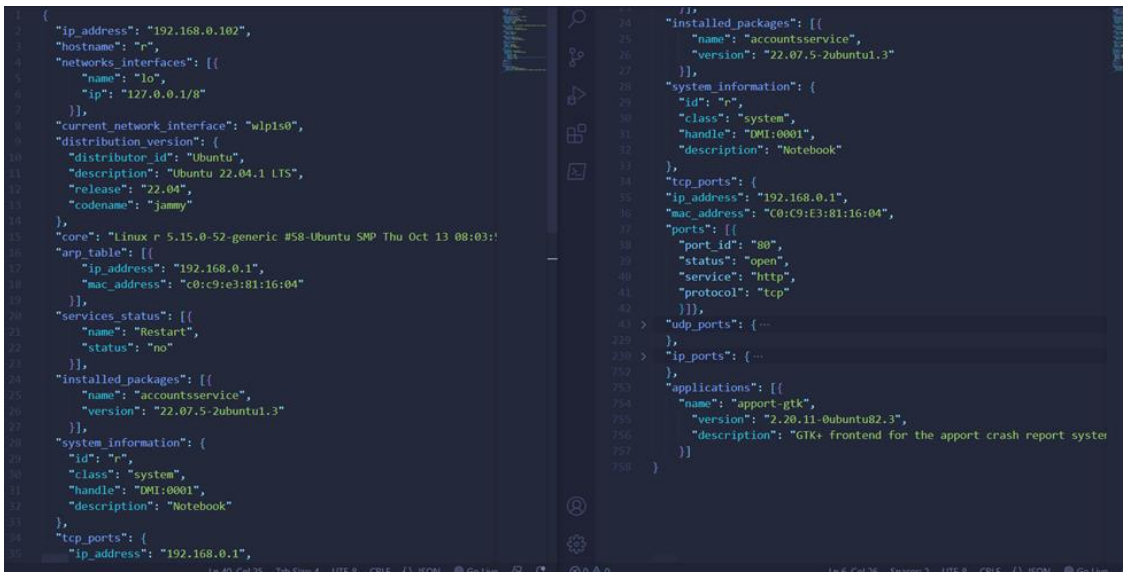


Рисунок 2 – Итоговый результат сервиса сбора данных

Сервис проведения атак. Данный сервис проводит атаки на основе информации, полученной от модуля сбора данных о системе. Исходя из данных, собранных с хоста и локальной сети, формируются цели, включающие в себя: IP-адрес, MAC-адрес, номер порта, статус порта информация о сервисе, на котором работает порт, протокол порта. Далее модуль проверяет узел на подверженность следующим атакам:

- SYN-флуд,
- UDP-флуд,
- ARP-спуфинг,
- атака «грубой силой»,
- истощение ресурсов DHCP,
- подмена DHCP-сервера.

Результатом выполнения атак является файл, куда записываются вектора атак со следующими параметрами:

- target – цель, на которую будет производиться атака,
- status – индикатор успешности атаки.

На рисунке 3 представлен результат векторов атаки.

Рисунок 3 – Верификация атак

Для автоматической проверки успешности атаки в данном сервисе используется верификация атак, которая представляет собой сниффер для каждого протокола. Принцип работы заключается в том, что атака и соответствующий ей сниффер запускается в двух параллельных потоках.

Сниффер перехватывает весь сетевой трафик, выбранного соответствующего протокола, который исходит из ключевого узла и корневого маршрутизатора.

После окончании атаки именно сниффер, анализируя перехваченный дамп сетевых пакетов, определяет успешно или неуспешно произошла атака и ставит булевое значение в итоговом файле в поле status, истина, если атака успешна, ложно, если не успешна.

В качестве примера на рисунке 4 приведен алгоритм работы сниффера для атаки истощение ресурсов DHCP.

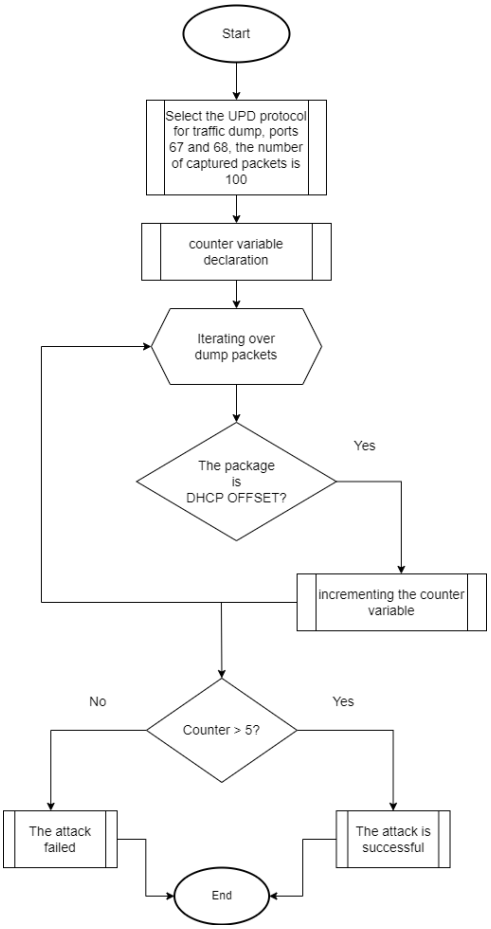


Рисунок 4 – Алгоритм работы DHCP-сниффера

В зависимости от того, какие атаки были выполнены с успехом, делается вывод о степени безопасности КИИ.

Веб-интерфейс. После тестирования работы сервиса локально был разработан веб-интерфейс для упрощения работы пользователя с сервисами. При работе с сервисами сначала на сайте пользователю будет предложено скачать скрипт, который собирает информацию о системе. Затем после того, как скрипт соберет информацию, пользователю будет предложено выбрать вектора атак, которые актуальны для его системы, и проверить их. На рисунке 5 представлен веб-интерфейс сервиса при поиске атак.

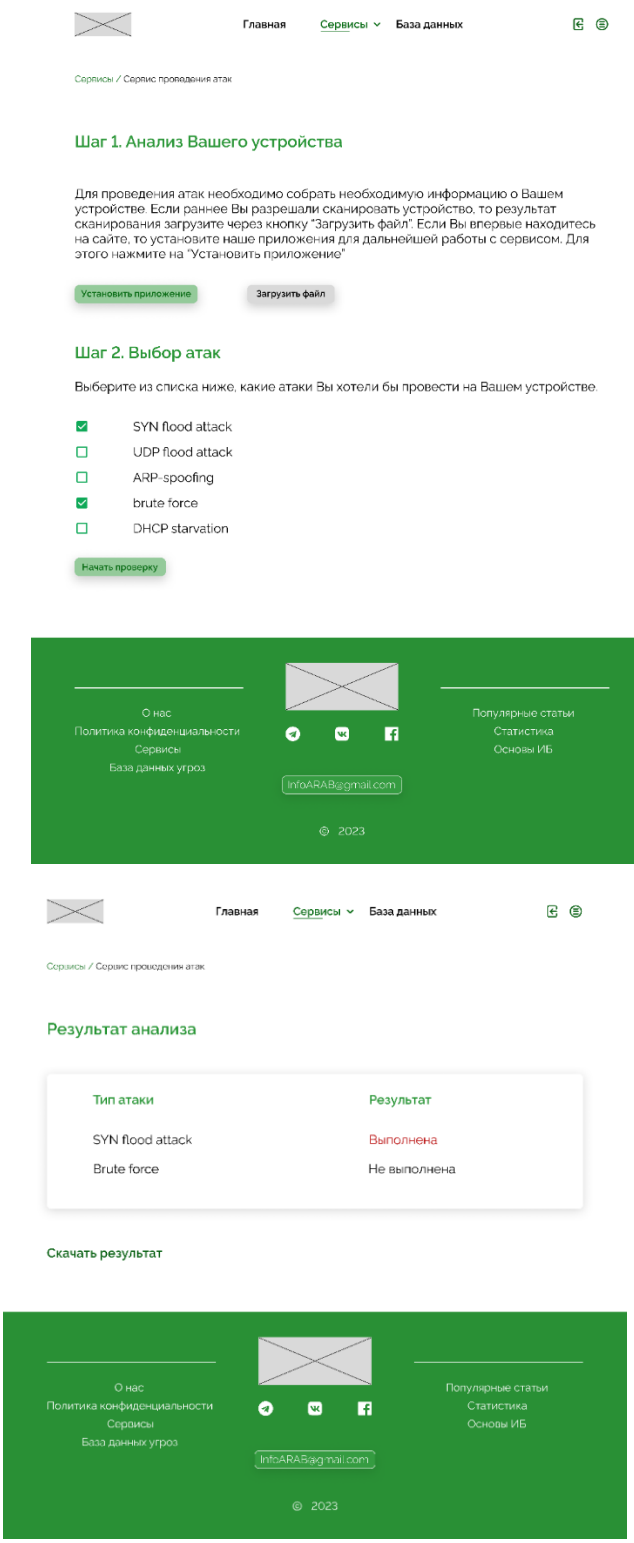


Рисунок 5 – Веб-интерфейс сервиса

Заключение. В заключение хотелось бы отметить, что всеобъемлющего и универсального метода тестирования для всех КФС не существует. В ходе исследования была разработана методика тестирования с учетом проведенного анализа и исследования взаимосвязи уязвимость–угроза–атака.

Данная методика не покрывает весь спектр атак, но позволяет тестовыми испытаниями сделать систему устойчивой на хрупкость, надежность (отказоустойчивость) и проникновение.

Кроме того, для преодоления проблем, с которыми сталкиваются существующие испытательные стенды, будущие исследования должны включать следующие цели.

Во-первых, это сверхбольшой масштаб. Благодаря развитию теорий сложных систем появляется много новых свойств, когда система достигает определенного масштаба и уровня сложности. Большинство современных испытательных стендов подходят только для небольших или средних КФС. Поэтому будущие работы должны быть направлены на расширение испытательных стендов, подходящих для сверхсложных испытаний КФС.

Во-вторых, несколько сценариев атак: большинство существующих тестовых площадок, ориентированных на тестирование безопасности, могут реализовать только некоторые общие сценарии кибератак для конкретной КФС. В будущем необходимо разработать тестовый стенд, который может одновременно реализовывать несколько сценариев атак для нескольких разных систем.

Наконец, многоцелевой охват проверки. Не существует испытательного стенда, который мог бы всесторонне проверить надежность, устойчивость и хрупкость КФС. По-видимому, в будущем разработка испытательного стенда для эффективного многоцелевого тестирования, включая одновременное функциональное и нефункциональное тестирование, станет активной областью исследований. Это может быть достигнуто путем интеграции передовых новых технологий, таких как интернет вещей, больших данных, облачных вычислений и искусственного интеллекта.

Работа выполнена при поддержке Совета по грантам Президента Российской Федерации. Стипендия Президента Российской Федерации молодым учебным и аспирантам (Конкурс СП-2022) № СП-858.2022.5.

Список источников и литературы:

1. Soupionis, Yannis and Thierry Benoist. «Cyber-physical testbed - The impact of cyber-attacks and the human factor» 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (2015): 326-331.

2. Tigist Abera, N. Asokan, Lucas Davi, Jan-Erik Ekberg, Thomas Nyman, Andrew Paverd, Ahmad-Reza Sadeghi, and Gene Tsudik. 2016. C-FLAT: Control-Flow Attestation for Embedded Systems Software. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 743-754. https://doi.org/10.1145/2976749.2978358

3. Chen, D.D., Woo, M., Brumley, D., & Egele, M. (2016). Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. Network and Distributed System Security Symposium.

4. Yosef Ashibani, Qusay H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Computers & Security, Volume 68, 2017, Pages 81-97, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.04.005.

5. R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, «Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid» in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sept. 2015, doi: 10.1109/TSG.2015.2432013.

6. Ashok, Aditya et al. «Experimental evaluation of cyber-attacks on Automatic Generation Control using a CPS Security Testbed». 2015 IEEE Power & Energy Society General Meeting (2015): 1-5.

7. R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, «Analyzing the cyber-physical impact of cyber events on the power grid» IEEE Trans. Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sep. 2015.

8. R. Liu and A. Srivastava, «Integrated simulation to analyze the impact of cyber-attacks on the power grid» 2015 Workshop on Modeling and Simulation of

Cyber-Physical Energy Systems (MSCPES), Seattle, WA, USA, 2015, pp. 1-6, doi: 10.1109/MSCPES.2015.7115395.

9. Yaacoub JA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocess Microsyst. 2020 Sep;77:103201. doi: 10.1016/j.micpro.2020.103201. Epub 2020 Jul 8. PMID: 32834204; PMCID: PMC7340599.

10. M. Cho, H. Jin, D. An and T. Kwon, «Evaluating Code Coverage for Kernel Fuzzers via Function Call Graph» in IEEE Access, vol. 9, pp. 157267-157277, 2021, doi: 10.1109/ACCESS.2021.3129062.

11. Shapiro, R., Bratus, S., Rogers, E., Smith, S. (2011). Identifying Vulnerabilities in SCADA Systems via Fuzz-Testing. In: Butts, J., Shenoi, S. (eds) Critical Infrastructure Protection V. ICCIP 2011. IFIP Advances in Information and Communication Technology, vol 367. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24864-1_5

12. An introduction to spike, the fuzzer creation kit. – URL: https://slideplayer.com/slide/248254/ (дата обращения 31.05.2023)

Вдовкина Екатерина Дмитриевна
бакалавр, МГТУ им. Н.Э. Баумана
E-mail: yekaterina.vdovkina@mail.ru

НЕОБХОДИМОСТЬ ПЕРЕХОДА К ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Аннотация. *В работе приведены потенциальные угрозы безопасности современных стандартов криптографии, выявленные в результате исследования уровня развития техники в области квантовых вычислений на начало 2023 года. Также перечислены схемы шифрования, не отвечающие стандартам безопасности в эру квантовых компьютеров.*

Ключевые слова: *постквантовая криптография, квантовая модель вычислений, дешифрование, кибербезопасность.*

Создание компьютера, реализующего квантовую модель вычислений (квантового компьютера), повлечет негативные последствия для множества криптографических механизмов. Проблема в том, что стойкость ряда распространённых криптографических схем обосновывается предположением о вычислительной сложности решения задачи факторизации больших полупростых чисел. И именно на квантовом компьютере можно эффективно реализовать с полиномиальной сложностью алгоритмы факторизации и дискретного логарифмирования в произвольной группе (метод Шора) , что в перспективе может привести к компрометации всех асимметричных криптографических схем, стойкость которых обосновывается предположением о сложности решения указанных задач, в том числе схем RSA, Диффи – Хеллмана и цифровых подписей ECDSA и ГОСТ Р 34.10–2012.

Ещё пару лет назад эксперты сходились во мнении, что достаточно большой для взлома RSA квантовый компьютер построят через десятки лет [1]. Дело в том, что опубликованный в 1994 году, алгоритм Шора позволяет факторизовать число N за полиномиальное время ($O(\log 3N)$), используя $O(\log N)$ кубитов [2]. То есть для факторизации числа N длиной

2048 бит, которое используется в качестве RSA-ключа, потребуется приблизительно 3000 кубитов. Это не представлялось возможным даже в ближайшее десятилетие, так как самый мощный на сегодня квантовый компьютер содержит 433 кубита и на его разработку ушли десятки лет. Однако в декабре 2022 года была опубликована работа, в которой исследователи из Китая, факторизовав 48-битное число на доступном им 10-кубитном квантовом компьютере, подсчитали, что масштабировать их алгоритм для использования с 2048-битными числами можно при помощи квантового компьютера всего лишь с 372 кубитами [3]. Прорыв обещан благодаря комбинированию алгоритма Шнорра [4] с дополнительным этапом «квантовой оптимизации» (Quantum Approximate Optimization Algorithm, QAOA). Такой компьютер уже создан компанией IBM, поэтому перспектива замены криптосистем по всему Интернету перестала быть чем-то отдаленным.

Более того, в январе 2023 года конгресс США принял закон, обязывающий все агентства начать переход к новым методам криптографии, которые не смогут быть взломаны квантовыми компьютерами. Данное решение на уровне государства лишь свидетельствует о том, что в новых подходах к безопасности есть острая необходимость.

Список источников и литературы:

1. Комарова Антонина Владиславовна, Коробейников Анатолий Григорьевич Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. №2 (30). URL: https://cyberleninka.ru/article/n/analiz-osnovnyh-suschestvuyuschih-post-kvantovyh-podhodov-i-shem-elektronnoy-podpisi (дата обращения: 12.04.2023).

2. Шор, Питер У. "Алгоритмы для квантовых вычислений: дискретные логарифмы и разложение на множители". Материалы 35-го ежегодного симпозиума по основам компьютерных наук. Ieee, 1994

3. Ян Б. и др. Разложение целых чисел на множители с сублинейными ресурсами на сверхпроводящем квантовом процессоре // Препринт arXiv arXiv: 2212.12372. – 2022.

4. Schnorr C.P. Efficient Signature Generation by Smart Cards. — J. Cryptology, 1991. — C. 161—174.

Жбанов Артем Михайлович
аспирант кафедры международных отношений и интеграционных процессов
факультета политологии МГУ им. М.В. Ломоносова
E-mail: norvejsky@gmail.com

КЛЮЧЕВЫЕ ФАКТОРЫ СТРАТЕГИЧЕСКОГО СДЕРЖИВАНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация. *Исследованы основные факторы стратегического сдерживания в информационной сфере. Рассмотрены перспективные механизмы оценки военно-политического потенциала государств. Определены понятия киберугрозы и кибервмешательства.*

Ключевые слова: *информационная сфера, киберпространство, кибербезопасность, международная информационная безопасность, информационное противоборство, интегрированные электронно-сетевые боевые действия, механизмы неядерного сдерживания.*

В условиях стремительного развития информационных систем и повсеместного проникновения интернет-коммуникаций вкупе с ростом влияния транснациональных цифровых гигантов – операторов данных миллиардов людей все более острыми становятся проблемы международного соперничества в информационном пространстве, военного применения интернет-технологий и распространение инструментов двойного назначения в интернете. Проблема милитаризации информационного пространства (киберпространства) прослеживается в доктринальных документах и структуре военного планирования США, в которых информационное пространство (киберпространство) является пространством возможного ведения боевых действий, а проведение военных операций и командование в информационном пространстве равнозначно таковым в области сухопутной, воздушной, морской и космической обороны [3, с.15]. При этом, борьба в информационном пространстве может иметь конкретные и серьезные последствия в материальном мире [2, с.19]. Аспекты военно-политического использования информационного пространства требуют от органов,

обеспечивающих государственную безопасность, новых подходов к стратегическому планированию и реагированию на возникновение потенциальных угроз.

Одним из методов предотвращения потенциальной угрозы является политика сдерживания. Стратегическое сдерживание предусматривает создание необходимой оборонной мощи государства, проведение активной упреждающей политико-дипломатической деятельности и организацию информационного противоборства, а также поддержание военными средствами политико-дипломатических, экономических, информационных мероприятий по предотвращению действий, способных причинить ущерб национальным интересам государства [1, с.5].

В данном исследовании под сдерживанием будет пониматься комплекс прямых и непрямых мер по предотвращению деятельности потенциального противника, которая направлена на прямой или опосредованный ущерб национальным интересам государства.

На сегодняшний день в исследовательском сообществе идут дискуссии о применимости концепции сдерживания в отношении военного использования информационных технологий [4, с.8]. Однако сдерживание угроз в информационном пространстве (киберпространстве) упоминается в стратегиях национальной безопасности США за 2018 г. [5, с.21], а также за 2023 г. [6, с.14]. Кроме того, проявлением политики сдерживания можно характеризовать заявления официальных лиц-представителей НАТО о возмездии при определенных действиях в информационном пространстве. В частности, Генеральный секретарь НАТО Йенс Столтенберг неоднократно заявлял о возможности применения статьи 5 устава НАТО в случае кибератаки на страну-члена Североатлантического альянса [7].

Как в случае с военно-политическим сдерживанием в отношении конвенциональных военных действий, сдерживание в информационном пространстве может применяться с помощью пассивных и активных действий.

Пассивное сдерживание представляет собой комплекс мер и инструментов по реализации возмездия в отношении враждебных действий, зафиксированных на уровне официальных государственных документов. Также к пассивному сдерживанию можно отнести увеличение военного потенциала государства посредством развития военно-технологического комплекса и увеличения численности и оснащенности вооруженных сил. В случае киберпространства к средствам пассивного сдерживания можно отнести официальное закрепление действий в информационном пространстве, которые будут считаться актом агрессии. Действия в информационном пространстве в данном случае должны быть классифицированы и определены как в случае с враждебными действиями или актами агрессии в традиционных областях (суша, море, воздух и т.д.) для их недопущения посредством неизбежного возмездия.

Помимо этого, к механизму пассивного сдерживания можно отнести наращивание совокупного потенциала в информационном пространстве или т.н. «кибермогущества». Термин «кибермогущество» используется зарубежным академическим сообществом для описания совокупного потенциала государства по ведению разведывательных и военных операций, защите собственной информационной инфраструктуры и развитию технологий в информационном пространстве [8].

Средства и инструменты активного сдерживания гораздо более разнообразны и представляют собой направленные и координируемые государством действия в отношении потенциального противника. Основная задача инструментов активного сдерживания – добиться общего ухудшения потенциала противника в ходе длительных спланированных действий в экономической, административно-политической, научно-технологической отраслях, а также общественном мнении.

Среди наиболее применяемых на текущий момент инструментов активного сдерживания можно выделить: технологические санкции и ограничение доступа к технологиям; создание технологической зависимости в

области программного обеспечения, вычислительных компонентов (процессоров, чипов и другой микроэлектроники), средств связи и компьютерной техники, ИТ-продуктов (в т.ч. социальных сетей); препятствование распространению ИТ-продуктов потенциального противника на собственном и зарубежных рынках; информационные кампании по дискредитации технологических решений или ИТ-продуктов потенциального противника; хедхантинг высококвалифицированных и ключевых специалистов, а также управленцев в высокотехнологичных отраслях; подкуп или принуждение участников цепочек поставок технологий в третьих странах с помощью более выгодных контрактов не участвовать в сделках с предприятиями потенциального противника; использование лоббистских групп для продвижения собственных ИТ-продуктов на внутреннем рынке потенциального противника, а также провоцирование условий, в которых создание национальных ИТ-продуктов в государстве-потенциальном противнике представляется коммерчески невыгодным. Список можно продолжить, однако все из вышеперечисленного активно применяется США в отношении государств, которые демонстрируют потенциал и возможности в области развития собственных средств обеспечения информационной безопасности и демонстрируют высокий уровень т.н. «кибермогущества».

Архитектура пассивного сдерживания и применение инструментов активного сдерживания опирается на оценку факторов, которые позволяют определить характеристику совокупного потенциала, и главное – угрозы, которую может реализовать то или иное государство. В дальнейшем данные факторы будут именоваться факторами стратегического сдерживания в информационном пространстве.

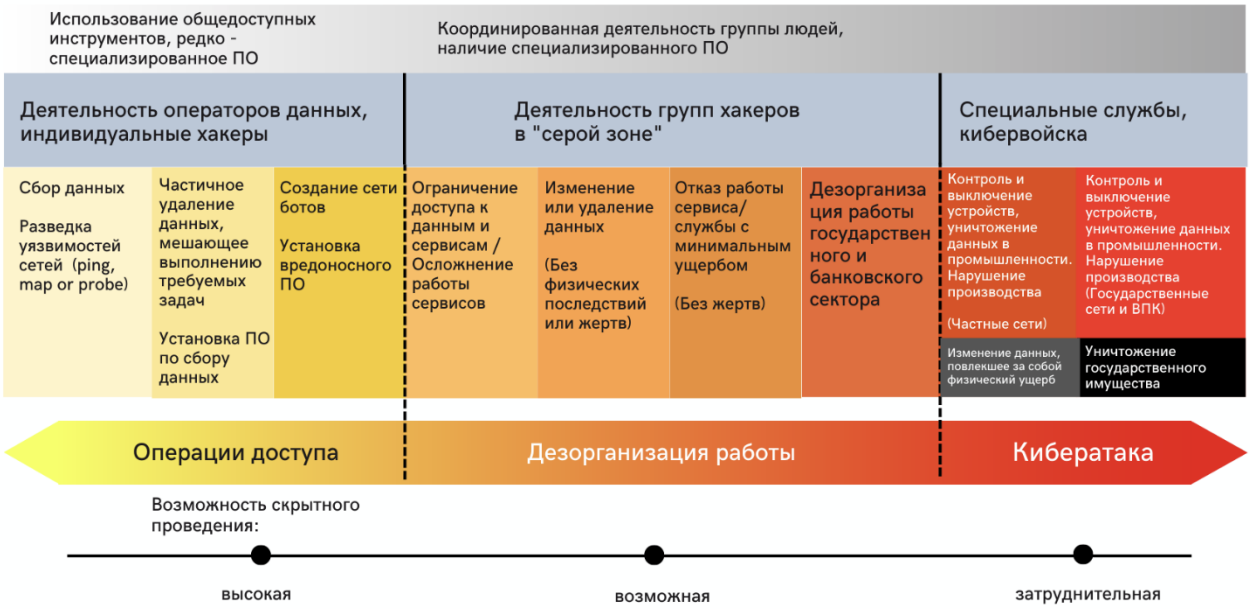
Прежде чем приступить к обзору факторов сдерживания, необходимо определить типы возможных действий, которые формируют архитектуру пассивного сдерживания посредством реагирования в информационном пространстве.

Прежде всего, стоит определить разницу в понятиях между кибервмешательством и кибератакой. Согласно определению, предложенному Центром НАТО по сотрудничеству в сфере кибероборонь, под кибератакой подразумевается операция в информационном пространстве, будь то наступательная или оборонительная, которая, как ожидается, приведет к ранению или смерти людей либо повреждению или разрушению материального имущества [9, с.91].

При этом стоит отметить, что по классификации центра НАТО по сотрудничеству в сфере кибероборонь, кибершпионаж и кража данных не являются кибератакой. Тем не менее, представители центра отмечают, что действия, которые не имеют последствий в виде материального ущерба, такие как кибершпионаж, могут иметь последствия на межгосударственном уровне[9]. Киберкомандование США классифицирует враждебные действия в информационном пространстве на три категории: операции доступа, операции, направленные на дезорганизацию, и непосредственно кибератаки [4, с.4].

В 2015 году Министр обороны США Эштон Картер заявил Комитету Сената по вооруженным силам, что «кибератака на критически важную инфраструктуру, экономику или военные возможности США» является «актом кибервойны», а также, что «кража интеллектуальной собственности с помощью кибернетических средств» ставит под угрозу национальную безопасность и экономическое процветание США [4, с.4]. Детализация классификации кибервмешательств Киберкомандования США представлена на рис.1.

Рисунок 1



Классификация кибервмешательств. Схема разаработана автором на основе данных Киберкомандования США. [4, с.5]

Система пассивного сдерживания посредством возмездия направлена на предотвращение кибервмешательств, которые относятся к кибератакам.

Факторы стратегического сдерживания в информационном пространстве можно разделить на следующие категории: политические, экономические, военные, технологические. При этом стоит отметить, что все из них необходимо принимать во внимание в совокупности, поскольку рассмотрение каждого из них по отдельности не предоставляет полноценное понимание потенциала представления угрозы со стороны потенциального объекта сдерживания. Политические факторы как в случае информационного пространства, так и в случае стратегического неядерного сдерживания практически идентичны и представляют собой набор субъективных и объективных факторов.

Политическими факторами являются: степень вовлеченности государства-потенциального противника в международные конфликты и характер этих конфликтов; место государства-потенциального противника в международной системе; проведение политики государства-потенциального

объекта сдерживания, противоречащей государственным интересам государства, осуществляющего сдерживание; форма политического режима, правления и государственного устройства; наличие государственной религии и степень религиозности населения; наличие государственной идеологии, уровень идеологического единства нации и характер государственной идеологии.

В целом политические факторы служат для идентификации государств-потенциальных противников, соперников и конкурентов на международной арене. В зависимости от позиции военно-политического руководства той или иной страны значимость конкретных политических факторов может уменьшаться или возрастать. Значимость данных факторов во многом зависит от понимания государством собственных национальных интересов и характера его международной стратегии, а также текущего состояния международной системы.

Экономические факторы стратегического сдерживания в информационном пространстве более разнообразны. При этом, анализ данных факторов должен учитывать, что многие коммерческие ИТ-продукты и решения могут иметь двойное назначение, и использоваться в случае возможного конфликта в качестве средства сбора данных, проводника информационной политики (в случае социальной сети), средства распространения вредоносного программного обеспечения и т.д.

Ключевыми экономическими факторами сдерживания в информационном пространстве являются следующие. Объем рынка национальных ИТ-решений и ИТ-продуктов в его ВВП; количество и объем капитализации национальных ИТ-предприятий, ведущих свою деятельность на международных рынках; объем услуг и продуктов национальных ИТ-компаний в общемировом сегменте рынка; объем услуг и продуктов национальных ИТ-компаний на рынке государства, осуществляющего сдерживание; объем услуг и продуктов национальных ИТ-компаний на рынке государства, осуществляющего сдерживание – данные факторы позволяют

определить общий уровень развития национальных компетенций в области информационных технологий, а также уровень потенциального доступа государства в киберпространстве на международном уровне, а также на уровне государства, осуществляющего сдерживание. При анализе указанных выше факторов, вместо ИТ-компаний, указанные выше экономические критерии также могут быть распространены на компании, осуществляющие производство технологических компонентов инфраструктуры информационного пространства, таких как устройства связи, смартфоны, компьютеры и их отдельных составляющих, такие как процессоры и материнские платы.

Военные факторы стратегического сдерживания в информационном пространстве определяют возможность государства вести наступательные и оборонительные операции в киберпространстве. Значимыми военными факторами являются характер военной доктрины государства, наличие отдельных доктрин или документов стратегического планирования в области информационного пространства, наличие специализированных подразделений органов государственной безопасности и вооруженных сил, направленных на ведение действий в информационной сфере и их численность.

Технологические факторы тесно связаны с экономическими, поскольку наличие конкурентоспособных разработок технологий и продуктов, связанных с киберпространством (к примеру, систем и средств связи нового поколения 5G) позволяет национальным компаниям производить и распространять свою продукцию за рубежом, косвенно распространяя область потенциального влияния государства. Кроме того, технологические факторы связаны с военными, поскольку наличие национальных технологических разработок предоставляет дополнительные возможности для использования их в военных целях или в разведывательных целях. К примеру, агентство национальной безопасности (АНБ) и федеральное бюро расследований США обязывают американские компании по разработке антивирусного

программного обеспечения не определять ряд программ-шпионов в качестве вредоносного ПО [9, с.17].

Среди технологических факторов можно выделить: объем производства процессоров, микросхем, систем связи и вычислительных устройств с доступом к сети интернет на территории государства и их уровень их присутствия на международном рынке, объем затрат на НИОКР в области вычислительных технологий и т.д.

Многие из данных факторов могут оцениваться в количественных показателях, часть из факторов должна оцениваться посредством экспертной оценки. Представляются целесообразными анализ и оценка данных факторов при реализации мер государственной политики по обеспечению информационной безопасности.

Проведенный анализ продемонстрировал необходимость дальнейших исследований в области сдерживания в информационной сфере. В частности, полагается целесообразной разработка комплексной системы оценки военного потенциала государств в информационном пространстве, которая может быть использована при подготовке документов стратегического планирования Российской Федерации.

Список источников и литературы:

1. Бартош А. Сдерживание в военных конфликтах XXI века. – М.: Горячая линия – Телеком, 2022

2. Scaparotti C.M., Cyberspace operations doctrine, Joint chiefs of staff, 2013. [Электронный ресурс] URL:https://irp.fas.org/doddir/dod/jp3_12r.pdf (дата обращения 30.05.2023)

3. Libicki M.C., Cyberdeterrence and cyberwar, RAND corp for U.S. Air Force, 2009 [Электронный ресурс] URL: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (дата обращения 30.05.2023)

4. Timothy M. McKenzie, Is Cyber Deterrence Possible? Air University Press, 2017 [Электронный ресурс] Источник: https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF (дата обращения 30.05.2023)

5. National cyber strategy of the United States of America, 2018 [Электронный ресурс] URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения 30.05.2023)

6. National cybersecurity strategy of the United States of America, 2023 [Электронный ресурс] URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (дата обращения 30.05.2023)

7. REUTERS, «Massive cyber attack could trigger NATO response: Stoltenberg», 2016 [Электронный ресурс] URL:https://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE (дата обращения 30.05.2023)

8. Voo J., Hemani I., Cassidy D., National Cyber Power Index 2022 – report Harvard Kennedy School, 2022 [Электронный ресурс] URL: https://www.belfercenter.org/publication/national-cyber-power-index-2022 (дата обращения 30.05.2023)

9. NATO CCDCE, Tallin manual on the international law applicable to cyber warfare, 2009 [Электронный ресурс] URL: http://csef.ru/media/articles/3990/3990.pdf (дата обращения 30.05.2023)

10. Lawton, G. Invasive Software: Who's Inside Your Computer? Pace University. [Электронный ресурс] URL: https://web.archive.org/web/20110720024630/http://utopia.csis.pace.edu/dps/2007/jkile/2005%20-%20Spring/DCS823/Spyware/01016895.pdf (дата обращения 30.05.2023)

Овчинников Святослав Сергеевич
аспирант, факультет государственного управления,
МГУ имени М.В. Ломоносова
E-mail: oss-009@mail.ru

Овчинников Владимир Сергеевич
студент II курса,
кафедра международные отношения и международное право,
Дипломатической академии МИД России
E-mail: ovs200@mail.ru

РОЛЬ ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Аннотация**. В современном мире возникают проблемы обеспечения информационной безопасности определенного государственного органа и страны в целом. С возникновением новых информационно-коммуникационных и цифровых технологий появляются, с одной стороны перспективы для развития, а с другой вызовы и угрозы при их использовании (воздействие новых вредоносных хакерских программ, атаки вирусов-шифровальщиков, нарушение конфиденциальности персональных данных госслужащего, разглашение государственной тайны, возможности шпионажа, снижение качества предоставляемых государством продукций и услуг из-за стороннего вмешательства в государственные системы, сайты). На фоне всех этих преимуществ, вызовов и угроз обеспечения информационной безопасности, возникает проблема обучения государственного служащего и развития у него новой цифровой компетенции – «кибербезопасность». В качестве методологии исследования был выбран традиционный анализ документов. Были проанализированы официальные нормативно-правовые акты и научная литература по теме исследования.*

***Ключевые слова**: государственный служащий, кибербезопасность, обучение и развитие, информационная безопасность, государственное управление, цифровые компетенции, цифровые технологии, государственная гражданская служба.*

На международном уровне обеспечение кибербезопасности играет важнейшую роль. Учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортной продукции, особенно актуальным становится вопрос обеспечения должного уровня информационной безопасности страны в современном глобальном информационном мире [5]. Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления [9]. В приказе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.02.2022 N 143 «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» приводится перечень областей цифровых компетенций, в числе которых «кибербезопасность и защита данных» [4]. Правильно выстроенная в цифровом пространстве система позволит защитить данные от кибератак. Рассмотрим определения кибербезопасность. Согласно проекту концепции стратегии кибербезопасности Российской Федерации: «Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [3]. Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства) [3]. Кибербезопасность (или безопасность

киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве [6]. В свою очередь, киберпространство — это сложная среда, возникающая в результате взаимодействия людей, программного обеспечения и услуг в интернете с помощью технологических устройств и подключённых к нему сетей, которые не существуют в какой-либо физической форме [6]. Сегодня мы сталкиваемся с резким увеличением количества компьютерных атак на российские информационные ресурсы, большая часть которых осуществляется с территорий иностранных государств [1]. Правительственная комиссия по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности протоколом от 18 декабря 2017 г. № 3 утвердила рекомендации о составе квалификационных требований компьютерной грамотности, необходимых для исполнения должностных обязанностей федеральными государственными гражданскими служащими [10]. Одна из которых включает знание основ кибербезопасности и обеспечение защиты информации (установка сложных паролей на служебный адрес электронный почтовый, безопасности удаленного доступа, персональных данных и т.д.). Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М.С., Русанов А.А. в своей книге предлагают модель цифровых навыков кибербезопасности [8], которая направлена на подготовку специалистов в области обеспечения информационной безопасности. Сладкова Н. М., Ильченко О. А., Степаненко А. А., Шапошников В. А. в своей статье предлагают модель квалификационных требований по информационной безопасности для госслужащего [7].

Заключение. Эффективность и результативность государственного служащего, в области обеспечения информационной безопасности во многом зависит от уровня освоения и развития цифровой компетенции «кибербезопасность».

Список источников и литературы:

1. Бойко С. Международная информационная безопасность: новые вызовы и угрозы // Международная жизнь. 2022. № 11. С. 10-13.

2. Камолов, С.Г. Артемова П.В. Информационные технологии для государственных служащих: учебное пособие / Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Факультет управления и политики, Кафедра государственного управления и права. - Москва : МГИМО (университет), 2017. – 215 с.

3. Концепция стратегии кибербезопасности Российской Федерации: [Электронный ресурс]. URL: http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения 14.05.23).

4. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.02.2022 N 143 «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации».

5. Распоряжение Правительства РФ от 01.11.2013 N 2036-р (ред. от 18.10.2018) «Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014 - 2020 годы и на перспективу до 2025 года».

6. Стратегии кибербезопасности: аналитический отчет [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf (дата обращения 14.05.23).

7. Сладкова Н.М., Ильченко О.А., Степаненко А.А., Шапошников В.А. Особенности оценки компетенций по информационной безопасности

государственных и муниципальных служащих // Вопросы государственного и муниципального управления. 2021. № 1. С. 122-149.

8. Сухомлин В.А., Белякова О.С., Климина А.С., Полянская М.С., Русанов А.А. Модель цифровых навыков кибербезопасности / Фонд Лига интернет-медиа. 2021. 294 с. DOI 10.25559/e3858-3795-1033-h.

9. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

10. Фотина Л.В. Кадровая политика на государственной службе: учебник для вузов. Москва: Издательство Юрайт. 2023. 362 с.

Терехова Вера Сергеевна
бакалавр
Тюменский государственный университет
E-mail: verasergeevnaterekhova@yandex.ru

ДЕЯТЕЛЬНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ОБЕСПЕЧЕНИЮ НАЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье рассматриваются нормативно-правовые акты России и их основные парадигмы для обеспечения информационной безопасности страны. Раскрывается содержание Стратегии национальной безопасности и Доктрины информационной безопасности Российской Федерации, их ключевые принципы и пути преодоления новых вызовов в связи с меняющейся ситуацией в мире. Также освещаются современные проблемы и угрозы информационной безопасности, их классификация, статистика, методы и способы предотвращения.*

Ключевые слова: *национальная безопасность России, информационная безопасность России, нормативно-правовые акты, Стратегия национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, проблемы и угрозы в области информационной безопасности, кибератаки, защита информации.*

Нормативно-правовые акты РФ по обеспечению национальной информационной безопасности. Информация — объект как собственности государства, так и других акторов нуждается в обеспечении надежной безопасности. Защита информации включает в себя широкий спектр прав ее владельцев и граждан на свободный доступ к информации, в соответствии с Конституцией. Основу защиты информации, а также условия и критерии для обеспечения информационной безопасности разрабатывают органы государственной власти, опираясь на цели и задачи национальной безопасности России.

Необходимыми критериями для стабильности и развития государства являются обеспечение безопасного состояния от внешних и внутренних угроз, сопротивляемость попыткам внешнего давления и способность пресечения и ликвидации возникающих угроз, а также предоставление необходимых внутренних и внешних условий, гарантирующих устойчивое и всеобъемлющее развитие страны и ее граждан.

Национальная безопасность содержит все виды безопасности, содержащиеся в Конституции и законодательстве России. Ключевое положение национальной стратегии - оборона страны. В один из компонентов национальной безопасности входит информационная безопасность.

Информационная безопасность Российской Федерации является состоянием защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Политика России в области национальной безопасности формируется на основе «Стратегии национальной безопасности Российской Федерации», утвержденной Указом Президента Российской Федерации 02.07.2021 г. № 400. [2] Стратегия является основой долгосрочного планирования, включающая цели и задачи внутренней и внешней политики по реализации национальных интересов и приоритетов Российской Федерации в области обеспечения национальной безопасности.

На современном этапе политической обстановки современное мировое сообщество претерпевает изменения. Укрепление позиций новых стран-лидеров приводит к изменению мирового порядка и выработку новых принципов и правил мироустройства. Стремление Западных стран сохранить свою гегемонию приводит к ослаблению системы глобальной безопасности и усилению нестабильности в мире. Действия радикальных и экстремистских

организаций дестабилизируют как внутреннюю, так и внешнюю обстановку в разных сферах деятельности России, в том числе в информационной среде. Проведение Российской Федерацией государственной политики в области обеспечения национальной безопасности повышает как внутреннюю стабильность, так и укрепляет потенциал России на мировой арене.

Одним из основных факторов для развития роли Российской Федерации в мировом сообществе является стремление к технологическому лидерству (п.22). Также на современном этапе национальными интересами для России становятся критерии информационной безопасности, одним из которых является развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия (п.25 п.4). В Стратегии обозначено, что информационное пространство стало активно осваиваться как платформа для ведения военных действий (п.17), проводятся информационных кампаний, направленные на создание враждебного образа России (п.19) и растет число преступлений, совершаемых с помощью информационно-коммуникационных технологий (п.42). Манипулирование социально-экономическими проблемами России незаконными формированиями за рубежом и внутри страны способствуют развитию негативных социальных явлений, нарастанию межнациональных конфликтов путем подстрекательства в информационной сфере (п.20).

Стоит отметить, что в Стратегии сформулированы стратегические цели и основные направления обеспечения информационной безопасности, в том числе улучшение системы информационной безопасности; предотвращение военных конфликтов, которые могут возникнуть в результате применения ИКТ; защита интересов союзников России в информационной сфере; ликвидация информационно-психологического воздействия, включая воздействие, направленное на распространение ложных сведений и подрыв исторических основ и патриотических традиций, связанных с защитой Отечества; улучшение производства ИКТ с применением отечественных разработок. Также стратегической целью обеспечения информационной

безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Сопутствующим документом по обеспечению информационной безопасности является «Доктрина информационной безопасности Российской Федерации», введенная в действие Указом Президента РФ от 05.12.2016 N 646. [1] Доктрина является системой официальных взглядов на обеспечение национальной информационной безопасности Российской Федерации. В ней обозначены национальные интересы в информационной сфере, включающие создание системы информационного обеспечения для противодействия угрозам в информационном пространстве и защиты суверенитета Российской Федерации; обеспечение устойчивого функционирования информационной инфраструктуры и единой сети электросвязи Российской Федерации; увеличение отрасли информационных технологий и электронной промышленности; информирование до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по событиям в стране и мире.

В Доктрине введены ключевые информационные угрозы и состояние информационной безопасности. Одним из ключевых негативных факторов, влияющих на состояние информационной безопасности, является информационно-техническое влияние зарубежных стран на информационную инфраструктуру в военных целях. Также развивается деятельность организаций, которые реализуют техническую разведку в отношении российских государственных органов и расширяют деятельность специальных служб для оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в стране и подрыву суверенитета государства. Стоит отметить также и проблемы компьютерной преступности в кредитно-финансовой сфере,

растет число преступлений, направленных на нарушение конституционных прав и свобод человека. Одной из насущных проблем в сфере информационной безопасности является низкий уровень внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и продукции зачастую не имеют комплексной основы.

Современные проблемы и угрозы в области информационной безопасности: методы и средства их предотвращения. В условиях меняющегося миропорядка растет число угроз международной информационной безопасности. Сетевое пространство является уязвимой средой для разжигания незаконной и террористической деятельности, подрывающая стабильность в мировом сообществе. Из-за модернизирующихся кибератак информационная сфера находится под воздействием хакеров, террористов и хактивистов.

Главным принципом обеспечения информационной безопасности является защита и противодействие возникающим угрозам информационной среды, имеющим типологизацию, к ним относятся: организационные, физико-технические, информационные и программно-математические. Организационные угрозы выступают в виде хищения информации с целью кражи конфиденциальных данных как для раскрытия компрометирующих документов и подрыва репутации (доксинг), так и для получения материальной выгоды (фишинг). Физико-технические угрозы обусловлены проблемами с персональным обеспечением в информационной системе, а также с нарушением норм обработки и передачи информации. Информационные угрозы включают психологическое воздействие, манипуляции сознанием, кибертерроризм и информационные войны с целью

пропаганды своих идеологических или политических намерений для дестабилизации социальных настроений. К программно-математическим угрозам относят нарушение доступа к файлам и системе (DoS и DDoS атаки) или видоизменение информации (дефейс) для подрыва информационной безопасности организации по личным или политическим причинам.

По статистике по количеству кибератак в России на 2022 год пришелся 2921 случай, а в 2021 году – 2418, увеличившись на 21%. Наибольшее число состоявшихся киберинцидентов пришлось на госучреждения, за 2022 год их количество возросло более чем в 2 раза. Из-за массовых утечек данных злоумышленники активно используют доксинг: атаки хактивистов увеличились в том числе и на сектор СМИ (45%) и на транспортную отрасль (43%). Также в каждой второй (51%) успешной кибератаке на организации использовались шифровальщики. А именно: госучреждения (15%), промышленные предприятия (15%), медицинские организации (14%) и научно-образовательные учреждения (13%). [5]

Данные угрозы определяют методы по обеспечению информационной безопасности системы. Оперативное обнаружение кибератак достигается с помощью распределения угроз по вероятности реализации; создания списка потенциальных правонарушителей; анализа уязвимостей субъекта; использования технических средств выявления угроз, способствующие уменьшить случаи проявления несанкционированного доступа. Более того, синергия применения физической охраны и технической системы способны увеличить нахождение покушения на информацию.

Незаконный доступ к информационным системам осуществляется по двум видам каналов. К контролируемым каналам относятся: терминалы, средства представления и документирования информации, загрузки персонального обеспечения, технологические пульты и органы управления, а также внутренняя сборка аппаратуры. К неконтролируемым: машинные носители с данными, которые выносят за пределы организации и по внешним каналам связи.

Из-за большого количества пользователей, которые имеют доступ к информационной системе, необходимо образование встроенного контрольного механизма, а также на основании административного регламента, разделение доступа пользователей. Более того, структура защиты информации должна иметь многоуровневый и многовекторный характер, так как увеличение средств обеспечения защиты информации приводит к уменьшению возможностей киберугроз.

Тактика и защита информации Российской Федерации состоит из предупреждения и контроля над усилиями несанкционированного доступа; оперативного обнаружения и ликвидации незаконных действий; фиксации события; определения и устранения причины кибератаки, анализа и дальнейшего предотвращения угрозы. [3] В виду быстротечности и сменяемости информации в системе, а также анонимности нарушителя происходит повышение угроз информационной безопасности. Для ликвидации вмешательства нарушителя в операцию обмена информацией между частями информационной системой и сетью требуется использование средств выявления и устранения кибератаки.

В настоящее время особую роль играет информационное противоборство. Информационное влияние глобальной компьютерной сети Интернет затмевает сектор СМИ, так как количество пользователей увеличивается, а альтернативные информационные ресурсы позволяют получить актуальную информацию в онлайн режиме. По этой причине Интернет-ресурсы стали площадкой для информационного воздействия.

Информационные кампании, руководствуясь политическими целями, влияют на сознание и поведение людей, в следствие чего стала интерпретация событий, происходящие на постсоветском пространстве, западными СМИ. Они перекладывают ответственность за происходящее на Россию, не учитывая имеющийся ряд проблем государств, а также требование Российской Федерации как суверенного государства обеспечить свою безопасность и национальные интересы в связи с расширением НАТО. [4]

Заключение. В настоящее время Россия претерпевает ряд трудностей в информационной сфере, как и все государства мира в связи с растущей ИКТ-уязвимостью, однако, выработанный ряд мер по защите информационного пространства позволяет отражать киберугрозы и способствовать отстаиванию своих национальных интересов на мировой арене. Для защиты информационной сферы Российская Федерация проводит комплекс усилий, включающий улучшение системы информационной безопасности и создание безопасной среды проверенной информации. В том числе обеспечивается безопасность информационной инфраструктуры: устраняется деструктивное информационно-техническое влияние как на российские информационные ресурсы, так и на объекты критической информационной инфраструктуры, в том числе осуществляется противодействие экстремистским и террористическим организациям. Активно развивается механизм прогнозирования, выявления и предупреждения угроз, определение их источников и способов ликвидации. Следует отметить, что Россия заинтересована и готова развивать сотрудничество с иностранными партнерами в области обеспечения информационной безопасности.

Список источников и литературы:

1. Указ Президента Российской Федерации от 05.12.2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации. [Электронный ресурс].URL: http://www.kremlin.ru/acts/bank/41460

2. Указ Президента Российской Федерации от 02.07.2021 г. № 400. [Электронный ресурс].URL: http://www.kremlin.ru/acts/bank/47046

3. ФСТЭК. Методический документ Меры защиты информации в государственных информационных системах. URL:https://docs.cntd.ru/document/499083160?marker=6500IL

4. Штофер Л.Л. Информационная война как радикальная форма политической борьбы. [Электронный ресурс].URL: https://cyberleninka.ru/article/n/informatsionnaya-voyna-kak-radikalnaya-forma

5. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс].URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/?sphrase_id=244484

Тчанникова Ксения Игоревна
студентка 3 курса, специалитет
Российская академия народного хозяйства и государственной службы
При Президенте Российской Федерации
E-mail: ksenya.tchannikova@mail.ru

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОСМИЧЕКОЙ ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ МИЛИТАРИЗАЦИИ

Аннотация. *В статье рассмотрено информационное обеспечение безопасности космической инфраструктуры в контексте милитаризации. Проанализированы отдельные аспекты использования информационно-цифровой инфраструктуры как неотъемлемого элемента современных национальных вооруженных сил и фактора военно-политического баланса посредством спутникового вещания.*

Ключевые слова: *информационная безопасность, спутниковая связь, милитаризация космического пространства, информационные технологии, легитимность спутникового вещания*.

Вопрос обеспечения безопасности космической инфраструктуры набирает актуальность в связи с ростом опасности проведения информационных войн посредством средств спутникового вещания. Данный аспект не теряет свою актуальность из-за пробелов в международном праве, определяющих четкие положения по вопросу спутниковых систем как структуры двойного назначения. Так, например, Антонов А.И. в своей работе «Международно-правовое регулирование военно-космической деятельности» [1] дает оценку качеству и характеру распространения международных актов, связанных с ограничением военной деятельности в космическом пространстве. Автор приводит классификацию видов военно-космической деятельности в зависимости от степени их кодификации в международном праве, выделяя следующие разделы:

- разрешенные виды деятельности в космосе;

- запрещенные виды деятельности в космосе;
- нерегулируемые виды деятельности в космосе.

Последний пункт А.И.Антонов определяет как «серые зоны», то есть те пространства/объекты в космосе, нормативное регулирование которых на данный момент отсутствует, однако, они могут нести серьезную военную угрозу, например, создание и развертывание в космосе средств оптико- и радиоэлектронного подавления, а также создание, испытание и развертывание противоспутникового оружия. Стоит отметить, что спутниковые системы в большей своей степени направлены на прием и передачу информации, по этой причине нельзя исключать косвенного использования спутниковых систем одного вида в целях внедрения одного государства в деятельность другого посредством теле- и радиовещания.

Космическое пространство, к сожалению, до сих пор имеет недостаточное нормативное регулирование, что автоматически делает данную отрасль максимально уязвимой на правовом поле. Вопросы об информационной безопасности стали обыденностью для общества, но не в контексте космического пространства. По этой причине, изучая национальное законодательство, к примеру, Указ Президента Российской Федерации от 05.12.2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [2], мы не встретим положения ни о космосе, ни о спутниковых системах в целом, несмотря на взаимосвязь последних с аспектом информационной безопасности.

Рассматривая Указ Президента Российской Федерации от 02.07.2021 г. №400 «О стратегии национальной безопасности Российской Федерации» [3], вероятно, в силу его долгосрочного применения, положения о космосе и спутниковых системах имеются, однако не в контексте информационной безопасности:

– ст. 15 Стратегии говорит о космическом пространстве, как о новом «полигоне» размещения оружия;

– ст. 62 в целях обеспечения национальной безопасности и противодействия угрозам экономической безопасности предусматривает укрепление позиций в области освоения космоса.

Стратегия предусматривает целую главу, посвященную информационной безопасности, где, в свою очередь, мы можем наблюдать как косвенное определение технологий спутникового вещания как тревожный фактор в обеспечении «секьюрности»[1], к примеру, согласно ст. 49 «посредством использования информационно-коммуникационных технологий для вмешательства во внутренние дела государства», подрывая суверенитет, так и напрямую: ст. 55 «Использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования», повышающих уязвимость отечественных информационных ресурсов к зарубежному воздействию.

Стратегия в вопросе информационной безопасности определяет для себя важность формирования безопасной среды оборота достоверной информации, как задачу, и ставит перед собой цель обеспечения информационной безопасности посредством укрепления суверенитета Российской Федерации, что не так давно уже нашло отражение в национальном законодательстве. Кодекс Российской Федерации об административных правонарушениях [4] был дополнен ст. 13.47, которая устанавливает ответственность за нарушения правил использования на территории Российской Федерации спутниковых связей, которые находятся под юрисдикцией иностранных государств.

Так как мы рассматриваем и вопрос милитаризации, то важным документом является Соглашение «Об использовании систем спутниковой связи военного назначения и их дальнейшем совершенствовании», 2018 г. [5]. Документ регламентирует создание специальной системы спутниковой связи исключительно военного характера по вопросам взаимного содействия, защиты и планирования для участников Содружества Независимых

[1] Секьюрность от англ. *security* (безопасность), используется в контексте обеспечения информационной безопасности

Государств с помощью развертывания их национальных сегментов. Важным аспектом является п.3 ст.9, который гласит о невозможности передачи полученной информации в рамках Соглашения третьим лицам в отсутствие соответствующего письменного согласия Стороны, которая эту информацию предоставила.

На международном уровне наибольший вклад в развитие межгосударственного взаимодействия спутниковой связи внесли Международный союз электросвязи и Комитет по использованию космического пространства в мирных целях. Однако стоит отметить также важность и многосторонних соглашений, регламентирующих услуги спутниковой связи, которые в формате правового обычая регламентируют определенные аспекты в вопросах спутниковой связи. К примеру, сложился следующий, незакрепленный нормативно, перечень участников, осуществляющих спутниковую связь:

1) оператор спутника связи;
2) оператор сети связи;
3) дистрибьютер услуг связи.

Оператор спутника связи обеспечивает бесперебойное функционирование спутника и гарантирует исправность всех составных его элементов, посредством починки или же превентивных мер по предупреждению неисправностей.

Оператор сети связи пользуется услугами спутника связи и обеспечивает передачу информации, ее скорость и качество.

Дистрибьютер услуг связи, в свою очередь, – это лицо, принимающее сигнал спутника, посредством специального оборудования.

Данные лица осуществляют цепочку передачи информации: легитимность их действий регламентируется посредством специальных соглашений по космическому праву: Договор по космосу 1967 года [6], устав Международного союза электросвязи 1992 года [7] и принятых в 1982 году

«Принципах использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания» [8].

Положения данных актов определяют право государств и частных лиц осуществлять телевизионное вещание посредством систем спутниковой связи. Однако, говоря об информационной безопасности и защите суверенитета государств, важно отметить, что вопрос о юрисдикции осуществления спутникового вещания на территории государств остается открытым. Так, выделяется две теории распространения информации посредством спутниковых систем. Одна из них – теория свободного вещания: регламентирует право на непосредственное осуществление телевизионного вещания одним государством на территории другого, - другая же теория, предварительного согласия, такого права не дает и говорит о необходимости получения транслирующим государством разрешения от принимающего. Свободное распространение информации может затронуть суверенитет государства, о котором так часто упоминается в документах по обеспечению спутниковой связи, к примеру:

– Конвенция Международного союза электросвязи, 1998 г. [9] в своей преамбуле полностью признает за каждым государством суверенное право регламентировать электросвязь;

– Соглашение «О создании международной системы и организации космической связи «Интерспутник»», 1972 года [10] обозначило, что договаривающиеся стороны действуют в интересах развития международного сотрудничества на основе уважения суверенитета и независимости государств, исключая попытки вмешательства во внутренние дела государства;

– Лига Арабских государств, в частности Египет, как и Российская Федерация, в контексте информационной безопасности, говорит о воздействии вещания на сознание граждан, поэтому создает специальные органы по вопросам контроля, мониторинга и регулирования работы в том числе и спутниковых станций, посредством внедрения особого законодательства, предупреждающего попытки умышленного

распространения ложной информации на территории государства. За мониторинг данного процесса в Египте отвечают такие органы как Министерство информации, а также Министерство связи и информационных технологий. Несмотря на усилия, предпринимаемые арабскими государствами для сохранения своего суверенитета, например, посредством ежегодного проведения конференций, организуемых Арабским региональным центром кибербезопасности и Международным союзом электросвязи по вопросам, в частности, информационной безопасности . из практики нам известны случаи прямого нарушения суверенных прав Ирана спутниковыми системами Европейских стран. Последние, по заявлению Ирана, вмешались во внутренние дела государства через спутниковые телеканалы посредством трансляции новостных каналов, оппозиционного содержания. Иранское государство, предприняв попытку заглушить сигнал на своей территории, которая кончилась неудачно, заглушило спутник, оставив без вещания некоторые Европейские страны. Таким образом была создана правовая коллизия, так как, с одной стороны, действие Ирана правомерно, государство защищает свои суверенные права, но с другой стороны неправомерно, так как посредством глушения сигнала умаляются права других государств на прием и передачу информации. Несмотря на обращения в Международный союз электросвязи данный вопрос так и остался нерешенным, что позволяет сделать вывод о невозможности глушения самого спутника иностранного государства, пусть даже транслирующего неугодную информацию недобровольно принимающей стране. За счет данного пробела возрастает возможность внедрения государств в суверенитет других стран, влияние на сознание граждан посредством агитационных кампаний и предоставлении недостоверной и заведомо ложной информации о государстве, принимающем сигнал спутника.

Заключение. На основе проведенного исследования автор пришел к выводу, что необходимо урегулировать вопрос с «серыми зонами» космического пространства, а именно с космической инфраструктурой

двойного назначения, которая, в лице тех же спутников, способна милитаризировать космос и фактически нивелировать понятие «суверенного государства», и из проблемы информационной безопасности вырасти до национальной.

Список источников и литературы:

1. Антонов А.И. Международно-правовое регулирование военно-космической деятельности. *Вестник МГИМО-Университета*. 2012;(4(25)):190-197
2. Указ Президента РФ от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71556224/
3. Указ Президента РФ от 2 июля 2021 г. №400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/401325792/
4. Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 06.03.2022 №42-ФЗ [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_411057/
5. Соглашение об использовании систем спутниковой связи военного назначения и их дальнейшем совершенствовании, 2018 г. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/542659484
6. Договор о принципах деятельности государств по иисследованию и использованию космического пространства, включая Луну и другие небесные тела, 1967 г. [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml
7. Устав международного союза электросвязи, 1992 г. [Электронный ресурс]. – Режим доступа: https://base.garant.ru/2540944/

8. Принципы использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания, 1982 г. [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/artificial_earth_satellites.shtml

9. Конвенция Международного союза электросвязи, 1998 г. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1902034

10. Соглашение «О создании международной системы и организации космической связи «Интерспутник»», 1972 г. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1901803

Цыплухин Станислав Алексеевич
студент 3 курса бакалавриата
Факультета международных отношений, политологии и зарубежного регионоведения
Российский Государственный Гуманитарный Университет
E-mail: stas22102002@gmail.com

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ

Аннотация. *В данной работе анализу подвергаются действия государств, связанные с использованием информационно-коммуникационных технологий в военно-политических целях. Особенное внимание уделяется актуальности проблематики и необходимости фокусировки большего внимания на возможные негативные последствия в случае отказа от проработки компромиссных путей отказа от вредоносного использования новых технологий. В работе приводятся конкретные примеры и то, как такие деяния могут «эволюционировать» в будущем.*

Ключевые слова: *информационно-коммуникационные технологии, вредоносного использования новых технологий, информационная безопасность.*

В последние годы информационные технологии стали важнейшим фактором в общей системе безопасности для государства. Информационно-коммуникационные технологии (ИКТ) стали представлять собой возможную угрозу для международной стабильности [5].

Использование ИКТ в военно-политических целях может быть в следующих проявлениях [2]:

1. Борьба с системами управления и контроля объектами военной инфраструктуры;
2. Использование информационной среды с целью разрушения командной структуры противника;

3. Использование автоматизированных систем в разведывательных целях;

4. Военные действия с использованием электромагнитной и направленной энергии для контроля противника;

5. Использование средств стратегической коммуникации с целью дестабилизировать общественные настроения;

6. Подмена субъекта исполнения враждебного деяния с целью провокации ответных мер и т.д.

Выше перечислена лишь часть тех угроз и вызовов, которые могут быть реализованы злоумышленниками при помощи ИКТ. Авторитетные источники [4] указывают на тот факт, что на сегодняшний день около тридцати государств обладают инфраструктурными возможностями, которые позволяют нападать на объекты критической инфраструктуры. Эти и другие аспекты, способы противодействия им будут освещены в докладе по теме.

В ходе написания работы были использованы различные методы исследования. Основа теоретической части была оформлена при помощи системного анализа. Данный метод способствовал комплексному изучению материалов и вычленению важнейших аспектов из них. Метод наблюдения, в свою очередь, способствовал охарактеризовать текущую обстановку на международной арене касательно вопросов использования ИКТ в военно-политических целях, а также проследить инициативы и конкретные действия в области достижения консенсуса в правовом урегулировании в указанной области [1]. Помимо этого, в исследовании использовался метод моделирования. Необходимость в нем возникает при составлении прогнозов возможных итогов переговоров государств по вопросу регулирования и ограничения использования технологий с вредоносными целями.

Целью исследования стала необходимость детального освещения существующей проблемы, а как следствие выработка предложений о возможных путях урегулирования проблемных моментов в данной области.

В ходе исследования также проводится сравнение деятельности США и РФ в сфере использования ИКТ, приводится ряд исторических примеров вредоносного использования, а также анализируется возможные «пути отхода» от негативных последствий такого рода атак в будущем. [3]

Заключение. Проведенное исследование дает характеристику существующих угроз в использовании ИКТ и способы защиты интересов государства и его инфраструктуры. Дается развернутая теоретическая характеристика по тематике и приводятся существовавшие практические примеры применения ИКТ в военно-политических целях.

Список источников и литературы:

1. О запуске Специального комитета для разработки под эгидой ООН универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // МИД РФ URL: https://www.mid.ru/ru/foreign_policy/news/1423383/

2. Логика глобального противоборства в XXI веке: информационный детонатор // РСМД URL: https://russiancouncil.ru/analytics-and-comments/analytics/logika-globalnogo-protivoborstva-v-xxi-veke-nformatsionnyy-detonator/

3. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. – 2019. – №1. – С. 2-9.

4. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. – А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с.

5. Bazarkina D., Pashentsev E. Artificial Intelligence and New Threats to International Psychological Security // Russia in Global Affairs. 2019. No1. URL: https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security/

Шао Цзысюань
аспирант 3 курса, МГУ, Высшая школа культурной политики и управления в гуманитарной сфере (факультет)
E-mail: 619543842q@gmail.com

«ЦИФРОВАЯ ВАЛЮТА» КАК ПЛАТЕЖНАЯ РЕВОЛЮЦИЯ В КИТАЕ — ЭФФЕКТИВНАЯ МЕРА ПО ПРОДВИЖЕНИЮ БОРЬБЫ С КОРРУПЦИЕЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Аннотация. *Данная статья посвящена анализу цифрового юаня как платежной системы Китая. Автором проведен анализ истории развития цифрового юаня в Китае, изучение эффективности его использования в борьбе с коррупцией, а также обобщение и исследование цифрового юаня как современного электронного платежного инструмента с высочайшим уровнем безопасности.*

Ключевые слова: *Китай, цифровой юань, противодействие коррупции, информационная безопасность.*

Введение. В мире уже более десяти лет разрабатывается цифровая валюта благодаря постоянному развитию науки и техники. Китай является первой страной в мире, которая создала научно-исследовательский институт цифровой валюты, а цифровой юань разрабатывается в Китае уже более десяти лет. Цифровой юань имеет большое значение для обеспечения информационной безопасности, экономической безопасности, борьбы с коррупцией, мошенничеством и отмыванием денег. Цифровой юань основан на технологии блокчейн, которая имеет более высокий уровень безопасности. Цифровой юань имеет тот же правовой статус, что и наличные деньги. Благодаря возможности отслеживания цифровой юань удобен для юридического надзора и эффективно повышает информационную безопасность. Центральный банк может использовать систему больших данных для подробной записи процесса обращения цифровых юаней. После ее

полного продвижения он может более интуитивно и четко понимать поток наличных. Это имеет положительное значение для создания информационной безопасности и защиты от -коррупция в мире. Это мощная мера, способствующая развитию глобальной информационной безопасности.

Методология исследования – выявление отдельных кейсов для получения детализированной информации о «Цифровая валюта» как платежная революция в Китае – эффективная мера по продвижению борьбы с коррупцией и информационной безопасности.

Результаты исследования демонстрируют, что система «двухслойной работы» цифрового юаня и т.д. эффективно защищает пользовательскую информацию и препятствует ее запрещению или использованию без законного разрешения. Эта является эффективным инструментом в борьбе с отмыванием денег, коррупцией и другими видами преступлений. В отличие от наличных денег, цифровая валюта не обладает анонимностью – следует подчеркнуть, что для некоторых крупномасштабных экономических преступлений цифровой юань будет основываться на политике KYC (know your customer) (то есть полностью понимать своего клиента) (имеется в виду расширенная проверка владельцев счетов, которая используется чтобы предотвратить коррупцию на основе системы борьбы с отмыванием денег, понять законность источника средств) разделить цифровой кошелек юаня на несколько уровней, с одной стороны, цифровой юань будет учитывать потребности в конфиденциальности обычных людей, но в то же время время, это должно быть противодействие и устранение преступности, борьбы с отмыванием денег, финансированием терроризма, уклонением от уплаты налогов, или, другими словами, существуют другие аспекты управления движением капитала.Для достижения баланса, для поддержания способность бороться с преступлениями, для крупных платежей или денежных переводов, пользователи должны подать заявку на кошельки с реальным именем, прежде чем они смогут совершать крупные платежи.Если есть коррупция или взяточничество, система реального имени используется для отслеживания и расследования дел, и

соответствующая информация может быть предоставлена в помощь[3]. Что исключает возможность ее использования для противозаконных целей, таких как коррупция, телекоммуникационное мошенничество, отмывание денег, незаконный оборот наркотиков и терроризм. Однако следует отметить, что при выпуске физических юаней сегодня общественность все еще может получить полную анонимность, обеспечиваемую физическими деньгами. Личное право на анонимность не будет лишено из-за выпуска цифровых юаней. Управляемость системы цифрового юаня означает не полный контроль и доминирование, а предотвращение и контроль рисков, борьбу с коррупцией и другими видами преступлений, что является объективной необходимостью для обеспечения общественных интересов и информационной безопасности [2].

Заключение. Способность цифрового юаня отслеживать транзакции, которые невозможно отследить с помощью традиционных банкнот и наличных денег, делает цифровой юань эффективным инструментом в борьбе с коррупцией. Благодаря внедрению технологии блокчейн операции с электронными валютами могут быть записаны и отслежены, поэтому мошенникам трудно избежать контроля, а с точки зрения информационной безопасности он также эффективен в борьбе с отмыванием денег и мошенничеством.

Нельзя игнорировать антикоррупционную функцию цифрового юаня, но следует также отметить, что цифровой юань является лишь инструментом и нуждается в согласовании с другими механизмами.

Во-первых, цифровой юань не может устранить слабость человеческой природы: цифровая валюта не может устранить проблемы с информационной безопасностью и коррупцию от источника, потому что она не может устранить жадность людей. На этапе ввода в действие неизбежно, что некоторые регуляторы будут злоупотреблять цифровой валютой, что приведет к коррупции и утечке информации о цифровой валюте, В связи с этим необходимо усилить процесс законодательства о цифровом юане.

Во-вторых, цифровой юань не может радикально решить некоторые проблемы в системе и управлении: хотя «цифровой юань» может эффективно сдерживать «коррупцию» финансовых учреждений в процессе оплаты, он не может коренным образом решить проблему системной и управленческой коррупции. Без хороших институтов и управления очень трудно полностью искоренить коррупцию.

Цифровой юань — это новый способ оплаты, который отличается от традиционных форм валюты. Благодаря своему техническому превосходству и правовому положению он будет играть огромную роль в борьбе с коррупцией. Однако нынешняя «цифровая валюта» Китая по-прежнему имеет много недостатков и не может полностью искоренить «проблемы коррупции и информационной безопасности». Информационная безопасность и работа по борьбе с коррупцией — это общая атака всех элементов, она не может опираться только на одну технологию, но должна использовать различные средства и меры для создания целостной и устойчивой научной системы.

Список источников и литературы:

1. **中国新**闻网. **多地**试水发放数字人民币工资 专家建议普及关键在“**好用**” . (28.04.2023). https://m.chinanews.com/wap/detail/chs/zw/9998631.shtml

2. 人民资讯. 现行电子支付工具中 数字人民币用户隐私保护等级最高. （26.07.2023）.https://baijiahao.baidu.com/s?id=1739375853229664055&wfr=spider&for=pc

3. 央行数字货币如何助力治理腐败？深度了解数字人民币 (06.07.2023). https://mp.weixin.qq.com/s/qDUk-Tg9EVvvKhLr1yhEPg

СЕКЦИЯ 2

«ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ»

Ляшкевич Мария Васильевна
студент 4 курса факультета Международных отношений,
Санкт-Петербургский государственный университет
E-mail: mariia4701@gmail.com

ВЛИЯНИЕ ИСПОЛЬЗОВАНИЯ ИНСТРУМЕНТОВ МЕЖДУНАРОДНОГО ПОЛИТИЧЕСКОГО МАРКЕТИНГА В СОЦИАЛЬНЫХ СЕТЯХ НА ГЛОБАЛЬНУЮ И РЕГИОНАЛЬНУЮ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ РОССИЙСКО-УКРАИНСКОГО КРИЗИСА В ДЕКАБРЕ-АПРЕЛЕ 2022 Г.

Аннотация. *Международный политический маркетинг в социальных сетях является эффективным инструментом реализации силы в цифровом пространстве для достижения политических целей. Это обусловливается тем фактом, что транснациональный характер таких онлайн-платформ, их уникальные алгоритмы, позволяющие демонстрировать контент определенным аудиториям (целевым аудиториям), возможность получать обратную связь от ЦА и анализировать статистику маркетинговых кампаний в режиме онлайн обеспечивают формирование прямых связей не только с внутренней аудиторией государства, но также и внешней.*

Ключевые слова: *международный политический маркетинг, социальные сети, российско-украинский конфликт, информационные стратегии.*

Инструменты международного политического маркетинга изначально транспортировались из коммерческого маркетинга и видоизменялись в соответствии с требованиями политических целей. Однако на данный момент стали создаваться уникальные методы политического маркетинга, присущие только данной сфере, что демонстрирует формирование независимой сферы научного знания [1].

Характерная черта российско-украинского конфликта заключается в активном применении информационных технологий, в особенности социальных сетей, которые являются одними из самых гибких ресурсов

построения прямых связей между «производителем информации» и ее «потребителями».

Анализ роли таких онлайн-платформ проводился с декабря 2021 г., когда впервые на международном уровне стали звучать заявления о необходимости прекратить военные учения Российской Федерации до апреля 2022 г. [2].

Характерная черта российско-украинского конфликта заключается в активном применении информационных технологий. Это проявляется в ограничении распространения данных в медиа-пространстве, посредством Интернета и через другие каналы связей. Также можно отметить наличие черт информационной войны, выражающейся в росте количества недостоверной информации, распространяемой с целью дискредитации и ослабления позиции противников.

Таким образом, **актуальность** проблемы заключается в том, особую роль в информационном противостоянии играют социальные сети, которые являются одними из самых гибких ресурсов построения прямых связей между «производителем информации» и ее «потребителями».

Цель работы – определить роль инструментов применения международного политического маркетинга в социальных сетях в российско-украинском конфликте и определить их влияние на глобальную и региональную безопасность.

Основным **методом** исследования является контент-анализ: он применен при исследовании публикаций на площадках Twitter, YouTube, Instagram*, Facebook*, TikTok и пр.

Для проведения исследования была использована **литература**, посвященная политическому маркетингу, как иностранных, так и российских авторов, а также научные труды, позволяющие проанализировать мягкую и жесткую силу акторов-участников российско-украинского конфликта. В качестве **источников информации** использовались статистические данные, правила пользования платформами, а также публикации рассматриваемых

социальных сетей – Twitter, YouTube, Instagram*, TikTok, а также ряда региональных социальных сетей, таких как Вконтакте, Telegram и Wiebo.

В ходе анализа были выявлено, что в контексте данных событий активно используются следующие инструменты:

1. Формирование трендов в социальных сетях при помощи комментариев.
2. Хештеги.
3. Акторы влияния (инфлюенсеры).
4. Рекламные публикации.
5. Публикации с вирусным эффектом.
6. Подмена контента с целью обойти код социальных сетей.
7. И другие инструменты.

Таким образом, использование вышеперечисленных инструментов маркетинга позволяет достичь основные международные политические цели - формирование имиджа и позиционирования актора для укрепления своей позиции на международном поле; влияние на других акторов международных отношений для создания выгодных ситуаций и достижения необходимых решений; влияние на внутреннюю аудиторию акторов по вопросу их отношения к международной политике, проводимой этим актором; контроль и воздействие на формирование мировой повестки СМИ. Тем не менее, маркетинг является мягким инструментом информационного воздействия в киберпространстве, который сложно контролировать оппозиционной стороной. Знания о том, какие инструменты международного политического маркетинга используются, позволяют выстраивать контрстратегии в информационном противостоянии.

* Организация Meta признана экстремистской по решению суда, деятельность организации запрещена на территории Российской Федерации [3].

Список источников и литературы:

1. Недяк И.Л. Политический маркетинг. Основы теории/И.Л. Недяк - Издательство «Весь Мир», 2008 г. – 352 с

2. Россия начала новые военные учения вблизи границ с Украиной // Deutsche Welle URL: https://www.dw.com/ru/rossia-nacala-novye-voennye-ucenia-vblizi-granic-s-ukrainoj/a-60391277 (дата обращения: 30.02.2023).

3. РКН обязал СМИ маркировать Meta* как запрещенную организацию // РИА Новости URL: https://ria.ru/20220321/smi-1779361306.html (дата обращения: 24.06.2023).

Алина Серегина Арамовна
студент Российско-Армянского (Славянского) университета
Ереван, Армения
alinasereginaa@gmail.com

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ В АРМЯНСКИХ СМИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Аннотация. *В статье рассматривается процесс информационно-психологического воздействия СМИ на общество, в период «бархатной революции» в Армении 2018 года. Выявляются манипулятивные особенности освещения событий, которые негативно влияют на имидж России, российско-армянские отношения и информационную безопасность.*

Ключевые слова: *манипуляции в СМИ, информационная безопасность, информационно-психологическое воздействия, цветные революции.*

В наши дни социум потребляет большое количество информации, которая находится в открытом доступе на разных носителях. Это влечет за собой информационный кризис, проявляющийся в нахлынувшем потоке информации, которую общество не успевает обработать, критически оценить и попадает под его влияние. Информационный шум затрудняет восприятие социально важной информации и создает сиюминутный контекст. На подобное общество легче всего воздействовать и применить манипуляционные технологии, в этом преуспевают средства массовой информации. Е. Л. Доценко [2] в своей книге «Психология манипуляции: феномены, механизмы и защита» определяет манипуляцию как вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями, при этом указывает на следующие признаки этого понятия: 1) родовой признак психологическое воздействие; 2) отношение манипулятора к другому лицу как к средству достижения

собственных целей; 3) стремление получить односторонний выигрыш; 4) скрытый характер воздействия (как факта воздействия, так и его направленности); 5) использование психологической силы, игра на слабостях; 6) побуждение, мотивационное привнесение; 7) мастерство и сноровка в осуществлении манипулятивных действий [2].

Манипулятивные технологии применяются в СМИ с целью психологического, политического, коммерческого принуждения, с использованием эмоций человека. «...Природа манипуляции состоит в наличии двойного действия вместе с открытым сообщением манипулятор посылает адресату «закодированный» сигнал, надеясь на то, что этот сигнал разбудит в сознании адресата образы, нужные манипулятору. Это скрытое действие опирается на «неявное знание», которым обладает адресат, на его способность создавать в своем сознании образы, влияющие на его чувства, мысли и поведение. Искусство манипуляции заключается в том, чтобы направить процесс воображения по нужному руслу, но так, чтобы человек не заметил скрытого воздействия» [8].

СМИ используют информационные поводы и внушают высокий градус тревоги и панические настроения. Примером может служить опыт воздействия на общество выбросов, связанных с «цветными революциями». В конце XX – начале XXI вв. произошли мощные геополитические и социально-экономические вызовы, брошенные мировому сообществу, которые оставили глубокий отпечаток на многих сферах. Это активно сопровождалось повсеместным «импортом демократии», которое оказало влияние на возникновение феномена «цветных революций».

Термин, так активно употребляемый средствами массовой информации, возник и вошел в оборот относительно недавно, после публикации в 1993 г. книги Джина Шарпа «От диктатуры к демократии. Концептуальные основы освобождения» [1]. В работе американского автора совершенно ясно прослеживаются принципы и методы борьбы с недемократическими

режимами посредством ненасильственного свержения авторитарных правительств стран [3].

Революции стали называть «цветными» по причине того, что первые события данного характера содержали в своем названии цвет или цветок. Например, Оранжевая революция на Украине, Революция роз в Грузии, Тюльпановая революция в Кыргызстане, Пурпурная революция в Ираке, Шафрановая революция в Мьянме, Революция лотоса в Египте.

Однако, названия некоторых движений бывают не очевидными. Например, «Джинсовая» (Васильковая) революция в Беларуси в 2006 г. Данное название революция получила из-за СМИ, освещавших ход событий. Предполагается, что джинсы олицетворяли рвение народа к свободе. А также «Бархатная революция» в Армении, 2018 г. В 1989–1990 гг. в Восточной Европе журналисты ввели этот термин, означающий бескровную смену власти. Иначе «бархатную революцию» описывают как ненасильственную, но так ли это на самом деле? Статьи в армянском медиа-поле после и во время «бархатной революции» гласят об обратном. В них четко прослеживаются манипулятивные технологии и отношение манипулятора к другому лицу как к средству достижения собственных целей, как было упомянуто в книге Е. Л. Доценко. Это в свою очередь создает антироссийские настроения в обществе, что может расцениваться как угроза информационной безопасности.

В информационном издании «Радио Азатутюн» (Радио Свобода), которое направленно на армянское медиа-поле часто прослеживаются антироссийские выбросы. Так, например, в статье «Бархатная революция принесла с собой «громадные перемены» в общественно-политической жизни» [7] от 17.10.2018 опубликованы следующие строки: «Многое было передано России, из-за чего у Армении есть слабые места. Сейчас Никол Пашинян, на мой взгляд, делает попытку работать [с Россией] как равный с равным». Из этих слов следует, что Россия якобы притесняет суверенитет Армении, а «новые власти» постараются решить эти проблемы.

В информационном издании «МИА Новости Армении» в статье от 20.07.2018 под заголовком «Армяно-российские отношения после "бархатной революции": новые возможности или новые проблемы» [6] важно отметить следующие строки: «по сей день повестка армяно-российских двусторонних отношений остается "на уровне тостов"», «Позитивных ожиданий от России в армянском обществе очень мало», «официальная Москва годами обеспечивала внешнюю легитимность режима Сержа Саргсяна вопреки чаяниям и ожиданиям армянского народа». Из представленных строк следует, что Россия якобы занималась внутренней политикой Армении и удерживала ненавистный в обществе режим. Данные строки накаляют обстановку в обществе, выставляя Россию как кукловода, управляющего внутренними процессами Армении. Из этого следует, что «бархатная революция» в Армении якобы была необходима.

Также после «бархатной революции» издание «Радио Азатутюн» продолжает искажать действительность. В статье от 18.09.2020 «У России есть агенты практически во всех госструктурах Армении» [7] отмечается:

– В администрации президента России премьер-министру Армении Николу Пашиняну дали оперативный псевдоним «Борода» и внимательно отслеживают каждый его шаг.

– После «бархатной революции» 2018 года под особым контролем подчиненных генерала Чернова оказался премьер-министр Армении Никол Пашинян.

– источник из Еревана под оперативным псевдонимом «Кандидат» присылает в Москву «компроматы» на Пашиняна.

– Опасаться шпионских разоблачений «друзьям России» не приходится: Службу национальной безопасности (СНБ) Армении давно называют «филиалом Лубянки», а в руководстве идет постоянная кадровая чехарда, сопровождающаяся громкими скандалами.

Из данных строк следует, что Россия якобы занимается шпионской слежкой за первыми лицами Армении, продолжают управлять вектором развития политики Армении и не дает ей свободно принимать решения.

В статье информационного издания «Аравот» от 18.09.2020 под заголовком «Россия – традиционный, но не всегда надежный союзник Армении: доклад в США» [5] отмечается следующее:

– Российские амбиции и жесткая политика в евразийском регионе ведет к региональной нестабильности.

– Страх перед российским неоимпериализмом стал доминирующей проблемой при оценке среды безопасности в Евразии.

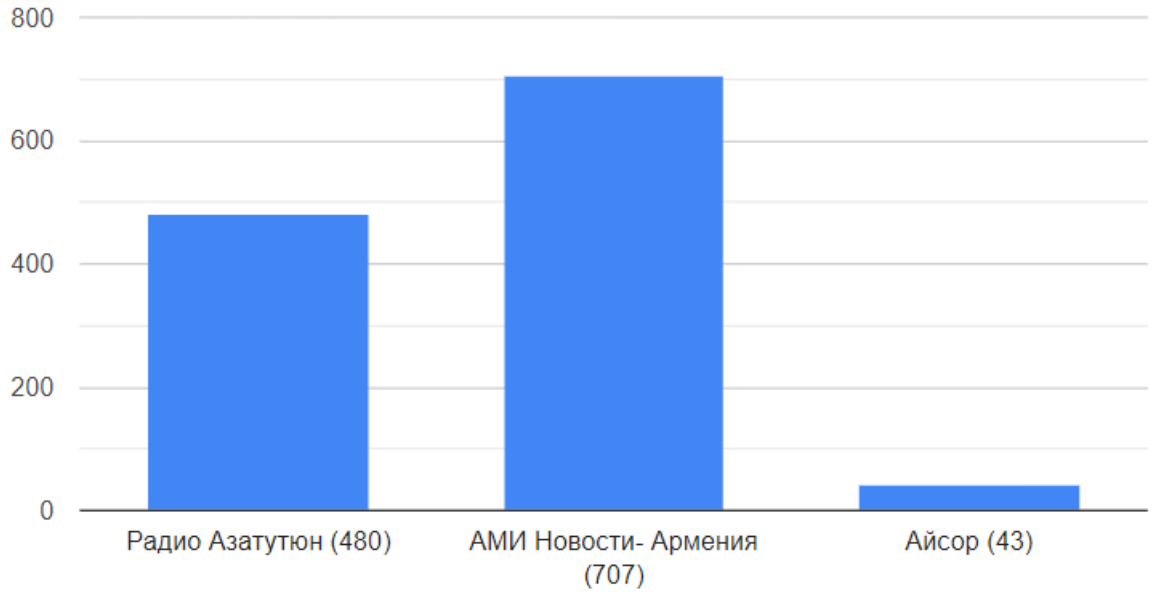
– В докладе говорится, что Армения, давний союзник России, например, сегодня имеет некоторые оговорки относительно надежности Москвы в качестве союзника. Эта тенденция особенно усилилась после бархатной революции.

– Россия остается непредсказуемой и агрессивной страной в Евразии, поэтому постсоветским странам следует тщательно взвешивать свои шаги и осторожно развивать отношения с Западом.

В данной статье использовался один из методов лингвистической манипуляции – использование эмоционально- экспрессивной лексики, например: Россия непредсказуемая и агрессивная страна, страх перед российским неоимпериализмом стал доминирующей проблемой, жесткая российская политика. А также идет призыв сближения отношений с Западом и подрыве армяно-российских отношений после «бархатной революции».

На диаграмме 1 «Количество упоминаний по тегу "бархатная революция"» представлен контент-анализ изданий «Радио Азатутюн», «АМИ Новости- Армения» и «Айсор» по тегу «бархатная революция», проведенный в мае 2023 года.

Диаграмма 1 «Количество упоминаний по тегу "бархатная революция"»



Из диаграммы 1 следует, что чаще всего тег «бархатная революция» упоминался в издании «АМИ Новости-Армения» - 707 раз. При этом в последних 100 статьях издания 45% материалов несут положительный характер по отношению к «бархатной революции», а 19% - отрицательный. В издании «Радио Азатутюн» за все время существования агентства тег «бархатная революция» упоминался 480 раз. В последних 100 статьях издания 21% материалов положительно описывали «бархатную революцию» и 7% - отрицательно. И лишь издание «Айсор» сохранял некий плюрализм мнений, 25% материалов положительно описывали «бархатную революцию», 23% - отрицательно из всех 43 статьей.

Как во время, так и после «бархатной революции» в Армении поднимались темы непродуктивных армяно-российских отношений. Россия в армянском медиа-поле выставлялась как агрессивная страна, имеющая прямое воздействие на принятие политических решений Армении. В следствии чего «бархатная революция» якобы была необходимым шагом для решения данной проблемы. Однако, ожидания общества после революции не оправдались, и в этом случае «Радио Азатутюн» выпустило материал о «российских шпионах», которые следят за первыми лицами Армении и снова вмешиваются в принятие решений.

Теме «цветных революций» отдельное внимание уделяют представители российских властей, подчеркивая сложные последствия «импорта демократии». Например, 14.04.2017 года в статье [4] «РИА Новости» президент РФ Владимир Путин заявил, что Россия не допустит возникновения «цветных революций» на своей территории и будет всячески способствовать предотвращению таких явлений на территории партнеров по ОДКБ. Также министр иностранных дел РФ Сергей Лавров неоднократно отмечал, «цветные революции» не сделали жизнь в странах бывшего СССР лучше, а лишь наоборот усугубили имеющиеся проблемы. [4]

Именно поэтому в новой Концепции внешней политики Российской Федерации [9] от 31.03.2023 имеется пункт 49, в котором упоминается пресечение «цветных революций»: «В целях дальнейшего преобразования ближнего зарубежья в зону мира, добрососедства, устойчивого развития и процветания Российская Федерация намерена уделять приоритетное внимание: предотвращению и урегулированию вооруженных конфликтов, улучшению межгосударственных отношений и обеспечению стабильности в ближнем зарубежье, в том числе пресечению инспирирования «цветных революций» и иных попыток вмешательства во внутренние дела союзников и партнеров России.

Заключение. Информационный кризис приводит к затруднению восприятия социально-важной информации, а также искажает картину действительности. Особенно это видно в медиапространстве Армении, во время и после «бархатной революции». В процессе убеждения СМИ прибегали к использованию языковых инструментов манипуляции. Примечательно то, что факт влияния манипуляции незаметен и трудно определим, а адресат сохраняет иллюзию самостоятельности сделанных выводов. Из этого в СМИ следовала идея необходимости «бархатной революции», которая не оправдала ожидания общества. Некоторые армянские СМИ выставляли Россию в качестве агрессивного государства, которое вмешивается во внутреннюю политику страны. Данное представление о России в армянском обществе ведет

к подрыву информационной безопасности. Такого рода «медийные атаки» трансформируют систему ценностей в армянском обществе, стереотипизируют сознание. Это создает послушный социум, который не в состоянии мыслить стратегическими категориями, подверженный легкому манипулированию. Данная проблема формирует новый запрос как для органов государственной власти, так и для всего общества в создании практических действий против медиа-манипуляций.

Список источников и литературы:

1. Джина Шарпа. От диктатуры к демократии. Концептуальные основы освобождения, 1993 URL: https://www.nonviolent-conflict.org/wp-content/uploads/2003/01/From-Dictatorship-to-Democracy-Russian.pdf
2. Доценко, Е.Л. Психология манипуляции: феномены, механизмы и защита / Е.Л. Доценко. - М.: ООО «Черо»: Юрайт, 2000. 342 с.
3. Журнал «Международные коммуникации», Издание Факультета международной журналистики МГИМО МИД России URL: https://intcom-mgimo.ru/2018/2018-09/color-revolution-phenomenon
4. Информационное агентство «РИА Новости» URL: https://ria.ru/20170412/1492073208.html
5. Информационное издание «Аравот» URL: https://www.aravot-ru.am/2020/09/18/336335/
6. Информационное издание «МИА Новости Армении» URL: https://newsarmenia.am/news/analytics/armyano-rossiyskie-otnosheniya-posle-barkhatnoy-revolyutsii-novye-vozmozhnosti-ili-novye-problemy/
7. Информационное издание «Радио Азатутюн» URL: https://rus.azatutyun.am/a/29549168.html
8. Кара-Мурза С.Г. Манипуляция сознанием. М.: Эксмо, 2005. С. 99
9. Официальное интернет-представительство президента России URL: http://www.kremlin.ru/events/president/news/70811

Эндже Ильдаровна Хаерова
студент,
федеральное государственное бюджетное образовательное учреждение
высшего образования «Казанский национальный исследовательский
технический университет им. А.Н.Туполева-КАИ»
E-mail: engikhaer@gmail.com

ОБНАРУЖЕНИЕ ПОДДЕЛЬНЫХ НОВОСТЕЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ LSTM

***Аннотация**. В ходе работы были изучены методы обнаружения фейковых новостей с помощью библиотеки обработки естественного языка (NLTK), методов Scikit Learn и Recurrent Neural Network, в частности LSTM. В процессе исследования были освещены этапы по обнаружению фальшивых новостей с помощью функции read_csv в Pandas. В данной работе приведен принцип работы данной системы.*

***Ключевые слова**: фейковые новости, библиотеки, RUN, LSTM.*

Учитывая тяжелые обстоятельства, с которыми мы все сталкиваемся в современном мире, новости играют довольно важную роль в нашей жизни. Мы в значительной степени полагаемся на него, чтобы узнать о различных областях, таких как здравоохранение, политика, образование, спорт и т. д. Но всегда существует проблема распространения и потребления ложных новостей. В настоящее время довольно часто люди не только верят ложным новостям, но и делают их менее склонными принимать настоящую информацию.

В этой статье рассматривается вопрос обнаружения фейковых новостей с помощью библиотеки обработки естественного языка (NLTK), методов Scikit Learn и Recurrent Neural Network, в частности LSTM.

Рекуррентная нейронная сеть (RNN) — это тип модели нейронной сети, в которой выходные данные предыдущего шага подаются в качестве входных данных для текущего шага. В традиционных нейронных сетях все входы и выходы независимы друг от друга, но в случаях, например, когда требуется

предсказать следующее слово предложения, требуются предыдущие слова и, следовательно, необходимо запомнить предыдущие слова. Так появилась RNN, которая решила эту проблему с помощью скрытого слоя [1].

Самая важная особенность RNN — это скрытое состояние, которое запоминает некоторую информацию о последовательности. RNN имеет «память», которая запоминает всю информацию о том, что было рассчитано. Он использует одни и те же параметры для каждого входа, поскольку выполняет одну и ту же задачу на всех входах или скрытых слоях для создания выходных данных. Это снижает сложность параметров, в отличие от других нейронных сетей (рис. 1).

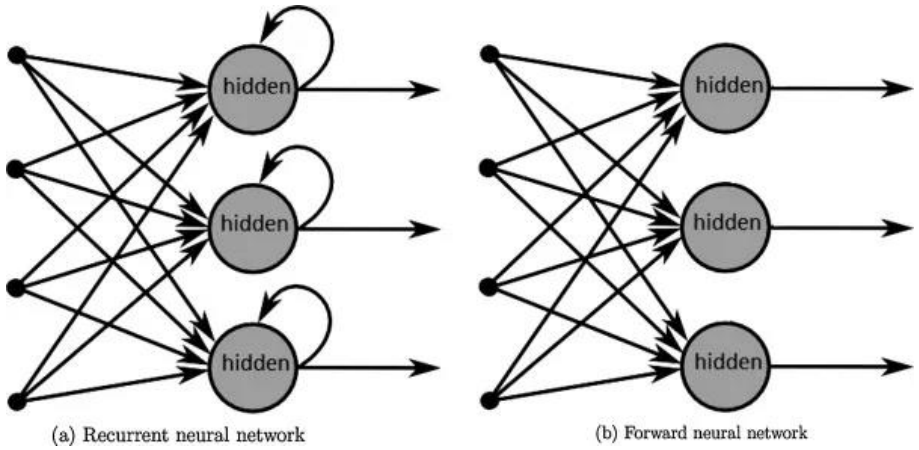


Рис. 1. RNN и FNN

Рекуррентные нейронные сети RNN не имеют состояния ячейки. У них есть только скрытые состояния, и эти скрытые состояния служат памятью для RNN. Это позволяет им сохранять информацию в «памяти» с течением времени. Но может быть сложно обучить стандартные RNN для решения задач, требующих изучения долгосрочных временных зависимостей. Это связано с тем, что градиент функции потерь экспоненциально затухает со временем (так называемая проблема исчезающего градиента) [1].

Сети LSTM — это разновидность RNN, в которой помимо стандартных единиц измерения используются специальные единицы. Блоки LSTM включают «ячейку памяти», которая может хранить информацию в памяти в течение длительного времени (рис. 2). Набор вентилей используется для

управления тем, когда информация поступает в память, когда она выводится, и когда она забывается [1].

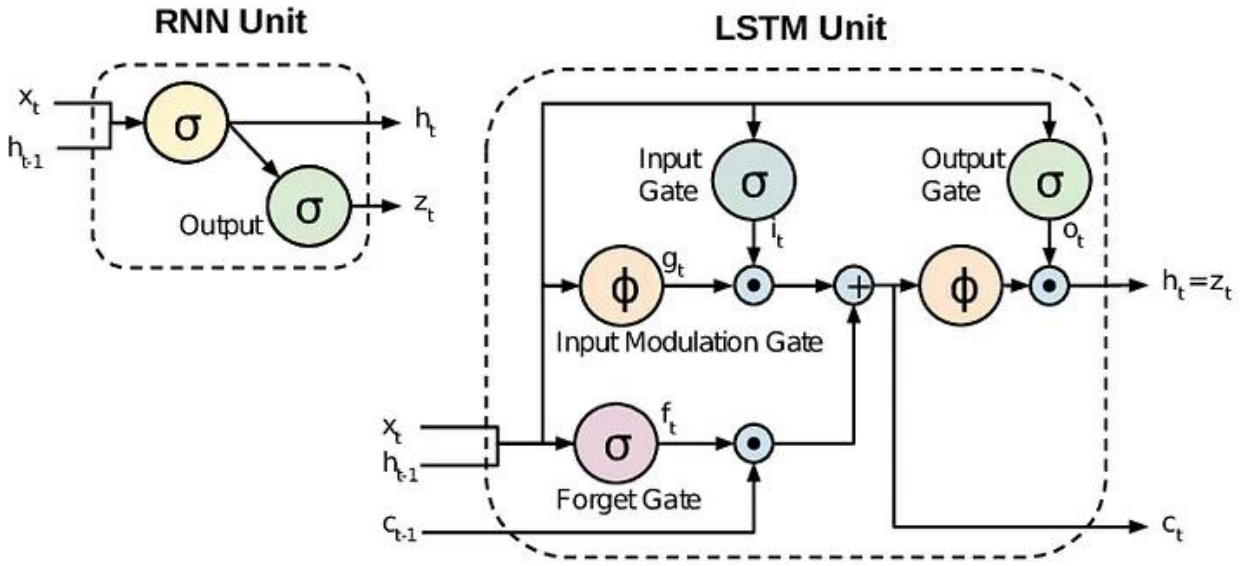


Рис. 2 RNN Unit и LSTM Unit

Первым шагом является очистка набора данных. Набор данных содержит некоторые пропущенные значения. Мы удаляем эти значения с помощью метода dropna. Также из набора данных мы видим, что столбец меток является нашей зависимой функцией, а все остальные — независимыми функциями. Поэтому мы разделяем эти независимые и зависимые функции и сохраняем их в переменных X и y соответственно [2].

```
#Отбрасывание значений NAN
df = df.dropna()
#Получение независимых признаков
X = df.drop('label',axis = 1)
#Получение зависимых признаков
y = df['label']
```

Напечатаем форму x и y.

```
печать (X.shape)
печать (y.shape)
```

Следующим шагом после очистки данных является предварительная обработка данных. Обработка данных — это просто преобразование

необработанных данных в значимую информацию посредством процесса. Он формирует основу для любых формулировок задач машинного обучения/глубокого обучения.

Импорт необходимых библиотек

```
import tensorflow as tf # для обучения глубоких нейронных сетей
из tensorflow.keras.layers import Embedding # для векторного представления с действительным знаком
из tensorflow.keras.preprocessing.sequence import pad_sequences # для фиксирования входной длины
из tensorflow.keras.models import Sequential # для создания последовательной модели
из tensorflow.keras.preprocessing.text import one_hot # для преобразования предложений в одноразовые представления с учетом размера словаря
из tensorflow.keras.layers import LSTM # для обработки последовательностей данных
из tensorflow.keras .layers import Dense #получает входные данные от предыдущего слоя
```

Следующим шагом является выделение корней и удаление стоп-слов из предложений. ***Стоп-слова:*** это слова, которые не добавляют смысла предложению. Мы удаляем эти стоп-слова из предложений для лучшего анализа. Примеры: {"а", "и", "то", "но", "как", "или", "что" и т. д.}

Стемминг: процесс удаления суффикса из слова и сведения его к корневому слову. Результирующее слово не всегда может быть осмысленным словом [2].

```
import nltk #библиотека НЛП
import re #regular expression
from nltk.corpus import стоп-слова #importing стоп-слова
nltk.download('stopwords')messages = X.copy()  #сохранение независимых функций
messages.reset_index(inplace = True) #так как значения NaN были удаленыfrom
```

```
nltk.stem.porter import PorterStemmer #Для создания основы
ps = PorterStemmer()
corpus = []      #list для встраивания
i в range(len(messages)):
review = re.sub('[^a-zA-Z ]',' ',messages['title'][i])  #для создания предложения только со словами в нижнем и верхнем регистре    #lower и разделение слов
review = review.lower().split()    # определение корней всех тех слов, которые не являются стоп-словами     review = [ps.stem(word) для слова в обзоре, если не слово в stopwords.words('english')]     review = ' '.join(review)
corpus.append(review)


corpus[0:10]   #печать первых 10 предложений после вывода
```

Таким образом, из приведенного выше вывода мы видим, что все стоп-слова были удалены, и в каждом слове предложений выполняется поиск корней.

Теперь нам нужно преобразовать текстовые данные (в корпусе) в одно горячее представление. ***One Hot Encoding:*** большая часть современного машинного обучения не может выполняться на категориальных данных. Вместо этого эти категориальные данные необходимо сначала преобразовать в числовые данные. Для выполнения такой операции используется одно горячее кодирование. По сути, это представление категориальных переменных в виде бинарных векторов. Эти категориальные значения сначала сопоставляются с целочисленными значениями. Затем каждое целочисленное значение представляется в виде двоичного вектора, состоящего из нулей. В нашем случае мы находим одно горячее представление каждого слова по отношению к размеру словарного запаса (вокабу) [2].

```
vocab=5000 #Настройка размера словаря
onehot_repr=[one_hot(words,vocab)для слов в корпусе]
onehot_repr
```

Как видно из вывода выше, первое слово в предложении 1 находится в индексе «950» словаря. Точно так же второе слово в предложении 1 находится в индексе «3189» словаря. Все нейронные сети требуют, чтобы входные данные были одинаковой формы и размера. Однако, когда мы предварительно обрабатываем эти данные и используем тексты в качестве входных данных для нашей модели LSTM, мы можем обнаружить, что не все предложения имеют одинаковую длину. Поэтому, прежде чем на самом деле передать эти предложения слою внедрения, мы должны сделать эти предложения фиксированной длины. Вот где «***заполнение***» становится необходимым. Здесь мы устанавливаем длину предложения равной 30 и выполняем заполнение этих горячих представлений предложений с помощью pad_sequences() [3]. Мы используем заполнение как «pre», что означает, что перед предложениями будут добавляться 0, чтобы сделать их одинаковой длины.

```
length = 30 #Установка длины предложения
embedded_docs=pad_sequences(onehot_repr, padding='pre',maxlen=length)
```

Создание модели LSTM

Перед созданием модели нам нужно определить количество векторов/признаков. Модель получает некоторый ввод в слое внедрения и преобразует его в определенное количество объектов/векторов. Поэтому в данном случае мы установили это число равным 40. Далее мы создаем последовательный объект для модели.

В 1-й слой добавляется встраивающий слой. На уровне внедрения первым параметром является размер словаря, за которым следует размер функции и, наконец, размер ввода, который в данном случае является размером предложения.

На следующем слое мы добавляем слой LSTM со 100 нейронами. Кроме того, поскольку это проблема классификации, добавляется плотный слой с функцией активации в виде сигмоиды [3].

Наконец, мы компилируем модель, используя функцию потерь в качестве двоичной кросс-энтропии (только два выхода), оптимизатор в качестве Адама и метрики в качестве точности.

```
#Создание модели lstm
embedding_vector_features=40
model=Sequential()
model.add(Embedding(vocab,embedding_vector_features,input_length=length))
model.add(LSTM(100)) #Добавление 100 нейронов lstm в слой
model.add(Dense (1,активация='сигмоид'))#Компиляция модели
model.compile(loss='binary_crossentropy',optimizer='adam',показатели"="['точность'])
```

Основная идея LSTM сети: Главным компонентом LSTM сети является состояние ячейки (a), которое проходит через всю цепочку подвергаясь лишь нескольким линейным преобразованиям. Удаление информации из состояния ячейки регулируется фильтрами (b), которые представляют собой слой сигмоидальной нейронной сети и поточечного умножения. Мы получаем точность ***90,85%*** для нашей модели. Таким образом, это указывает на то, что наша модель работала достаточно хорошо. Для сравнения фактических значений и прогнозируемых значений на тестовых данных по модели мы создали фрейм данных. Мы преобразовали тестовые данные (массивы) в список, а затем в словарь. Теперь кадр данных создается со словарем [1].

Принцип работы [1]:

1. LSTM определяет информацию, которую можно исключить из состояния ячейки.

2. Определяет новую информацию, которую стоит добавить в состояние ячейки.

3. Производит замену старого состояния на новое.

4. Решает вопрос, с тем какую информацию мы хотим получить на выходе.

Преимущества: отсутствие проблемы с обработкой долговременных зависимостей (по сравнению с RNN).

Недостатки: высокие затраты на вычисления, то есть более долгий инференс.

В наши дни методы детектирования искусственных новостей развиваются быстро, но это все еще очень сложная проблема, требующая дальнейшего изучения. Несмотря на отсутствие в настоящий момент однозначного определения понятия «фейк-ньюз», «фальшивые новости» набирают обороты и требуют дальнейшего изучения. Данная работа демонстрирует одно из возможных решений проблемы за счет методов определения этого типа новостей в социальных сетях, основанных на использовании систем с элементами искусственного интеллекта и машинного обучения.

Заключение. В ходе работы были подробно проанализированы существующие решения классификации новостного контента и текстовой информации, в частности. Также более подробно рассмотрены инструменты глубокого обучения, а именно слои нейронных сетей, которые используются для обработки текстовой информации.

Список источников и литературы:

1. Джаянты Кумар Пал. Обнаружение поддельных новостей с использованием нейронных сетей LSTM [Электронный ресурс] // Library.ru: информ.-справочный портал. М., 2021. URL: https://jayant017.medium.com/fake-news-detection-using-lstm-neural-networks-5bfb158be55e (дата обращения: 16.05.2023).

2. Федерика Монти, Фабрицио Фраска, Давид Эйнард, Дэймон Мэннион, Майкл М. Бронштейн. «Обнаружение фальшивых новостей в социальных сетях с помощью геометрической глубины обучение». 2019

3. Federico Monti, Fabrizio Frasca, Davide Eynard, Damon Mannion, Michael M. Bronstein. «Fake news detection on social media using geometric deep learning» 2019.

Чаморов Никита Михайлович
бакалавр 4 курса факультета
«Документоведение и архивоведение»
Донецкий государственный университет
E-mail: chamorow.n@yandex.com

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ И СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ХОДЕ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ

Аннотация. *Статья посвящена анализу использования социальных сетей и современных технологий в ходе ведения боевых действий, особенно в конфликте между Россией и Украиной. Рассматриваются как положительные, так и отрицательные стороны такого использования. В качестве примера приводится роль Telegram-каналов в информационном противоборстве и координации действий. Дана оценка использованию спутников и программных продуктов для успешного планирования боевых операций. В выводе дается общая оценка применения специального программного обеспечения силовыми ведомствами.*

Ключевые слова: *разведка, базы данных, социальные сети, большие данные, спутники.*

Современные войны и вооруженные конфликты требуют от сторон конфликта не только применения традиционных средств и методов ведения боевых действий, но и использования новых возможностей, предоставляемых информационно-коммуникационными технологиями. Одной из таких возможностей является использование социальных сетей и других Интернет-платформ для сбора, обработки, распространения и анализа информации об обстановке на месте, о действиях противника и своих сил, о потребностях пострадавшего населения и организаций, оказывающих ему помощь.

Использование социальных сетей и современных технологий в ходе ведения боевых действий имеет как положительные, так и отрицательные стороны. С одной стороны, это может способствовать повышению эффективности управления силами и средствами, ускорению принятия

решений, улучшению координации действий различных участников конфликта, увеличению точности поражения целей, снижению количества жертв среди гражданского населения и повышению его защищенности.

С другой стороны, это может создавать риски для безопасности и конфиденциальности информации, угрожать нейтралитету и независимости гуманитарных организаций, способствовать распространению дезинформации и пропаганды. Так, например, воюющие стороны могут анализировать фотографии и видео из профилей социальных сетей, а затем на основе собранных данных создавать всевозможные «deep-fake» видео- и аудиоматериалы для ввода в заблуждение населения и распространения панических настроений в обществе.

Поэтому использование социальных сетей и современных технологий в ходе ведения боевых действий требует от сторон конфликта соблюдения определенных правил и принципов, таких как проведение различия между военными и гражданскими объектами, запрет на причинение излишних страданий и чрезмерного вреда, уважение к человеческому достоинству и личной жизни, ответственность за свои действия и поступки, совершенные во время пребывания в рядах воинских подразделений.

С началом Специальной военной операции (СВО) telegram-каналы играют важную роль в боевых действиях между Россией и Украиной, начавшихся в феврале 2022 года. С одной стороны, они являются источником распространения противоречивой и неподтверждённой фактами информации для разных сторон конфликта, с другой – платформой для выражения мнений и позиций различных политических сил и лидеров. Среди самых популярных и влиятельных telegram-каналов, связанных с СВО, можно выделить каналы главы Чечни Рамзана Кадырова, пресс-службы бизнесмена и главы ЧВК «Вагнер» Евгения Пригожина, замглавы Совета Безопасности РФ Дмитрия Медведева, различных военных корреспондентов, находящихся в зоне СВО и в реальном времени сообщающих о ходе боевых действий и передвижении войск [1].

Если говорить о роли спутниковой разведки, то она играет важную роль в современной войне, поскольку позволяет получать оперативную и достоверную информацию о положении и действиях противника, а также обеспечивать связь и навигацию собственных войск. Спутники-радары могут проникать сквозь облака и темноту, отслеживая перемещение техники и людей на земле. Спутники-шпионы могут делать высококачественные снимки поверхности, раскрывая маскировку и обманные маневры врага. Спутниковые коммуникаторы могут передавать данные и команды между различными подразделениями, усиливая координацию и эффективность боевых действий. Спутники-навигаторы могут определять точное местоположение и скорость своих и чужих объектов, улучшая точность огня и мобильность войск.

Однако спутниковая группировка также подвержена угрозам со стороны противника, который может пытаться вмешаться в ее работу с помощью кибератак, помех, лазеров или противоспутникового оружия. Поэтому для обеспечения безопасности и устойчивости космической инфраструктуры необходимо развивать новые технологии, такие как вязаные антенны, защищенные сети или космические силы.

Если посмотреть на опыт использования спутниковой группировки в зоне СВО, то украинским вооруженным силам и разведывательным подразделениям большие массивы данных на постоянной основе предоставляет американская компания Maxar Technologies, являющаяся одним из лидеров в области спутниковой фотографии и аналитики.

Она предоставляет высококачественные снимки зоны российско-украинского конфликта, которые используют в своей работе как зарубежные и украинские СМИ, так и эксперты по безопасности, различные аналитические центры для составления отчетов и докладов.

С помощью снимков в высокодетализированном формате можно распознать расположение и передвижение военной техники, а также разрушения, нанесенные гражданской инфраструктуре и населению в ходе введения боевых операций. Компания Maxar сотрудничает с различными

международными организациями, в том числе с ООН, НАТО и правозащитными группами, чтобы обеспечить прозрачность и подотчетность в условиях активного конфликта.

Для успешного проведения боевых операций необходимо использовать соответствующее программное обеспечение. Так западные спецслужбы используют программного обеспечения, от компании Palantir. Один из наиболее интересных продуктов Palantir, который представляет интерес для силовых ведомств — Palantir Gotham. Данная программа представляет собой платформу с запатентованной моделью искусственного интеллекта для интеграции, управления и анализа разнородных данных из различных баз данных, таких как документы, фотографии, видео, звук, социальные сети, биометрия и другие. Palantir Gotham позволяет создавать совместные рабочие пространства для аналитиков, оперативников и командиров, где бы они все взаимодействовать друг с другом, выявлять скрытые связи и паттерны, прогнозировать угрозы и риски, грамотно планировать и координировать действия на основе собранных ранее данных [3].

Palantir Gotham используется в боевых действиях для поддержки разведки, контрразведки, спецопераций, кибервойны, контртерроризма и множества других задач. Например, с помощью Palantir Gotham американские военные могут отслеживать перемещения боевиков, определять места складирования оружия и взрывчатки, анализировать сети связи и финансирования террористов, выявлять потенциальные цели для ударов и рейдов. Также Palantir Gotham помогает военным координироваться с союзниками и местными силами безопасности, обмениваться данными и создавать единую картину боестолкновений в заданном секторе. Программа заранее может рассчитать результат проведения боевой операции благодаря симуляции действий в цифровом измерении.

Большие данные играют важную роль в современных боевых действиях, так как они позволяют анализировать и прогнозировать поведение противника, оптимизировать стратегии и тактики, улучшать эффективность

оружия и оборудования, а также снижать риски для собственных войск и мирного населения. Большие данные представляют собой огромные объемы информации, которые поступают из различных источников, таких как спутники, беспилотники, радары, камеры, датчики, социальные сети и другие. Для обработки и использования этих данных необходимы специальные алгоритмы, программы и вычислительные ресурсы. Большие данные могут помочь в решении различных задач на поле боя, таких как разведка, наведение, целеуказание для нанесения точного артиллерийского удара, координация и коммуникация между подразделениями, логистика для доставки боеприпасов в зону проведения боевых действий.

Необходимо отметить, что OSINT (разведка по открытым данным), имеет ряд преимуществ перед другими видами разведки, такими как HUMINT (человеческая разведка), SIGINT (сигнальная разведка) или IMINT (разведка по изображениям). Основные преимущества OSINT заключаются прежде всего в доступности, оперативности обновления данных, многообразии и низкой себестоимости. Открытые источники могут предоставлять большой объем информации в режиме реального времени, которая может быть проанализирована с помощью специального программного обеспечения и искусственного интеллекта. Необходимо также подобрать подходящие кадры с соответствующей квалификацией для качественного проведения OSINT-манипуляций. Открытые источники также могут дополнять и подтверждать информацию из других разведывательных каналов, переводить их на разные языки мира [2].

Однако OSINT также имеет свои ограничения и риски. Основные недостатки OSINT — это ненадежность, манипуляция и перегрузка информацией. Открытые источники могут содержать ошибки, устаревшие данные, ложную или предвзятую информацию, которая может быть использована для дезинформации и негативного влияния на общественное мнение. Открытые источники также могут быть перегружены избыточной или нерелевантной информацией, которая затрудняет поиск необходимых данных.

Кроме того, OSINT может быть подвержен контрразведке и противодействию со стороны противника.

Таким образом, OSINT играет важную роль в военном деле, но требует критического мышления, профессиональных навыков и сбалансированного подхода к анализу и использованию информации из открытых источников.

Заключение. Исходя из вышесказанного можно прийти к выводу, что современные источники информации могут помочь для проведения боевых операций, так и привести к провалу из-за дезинформации сведениями, которые не были заранее проверены и не прошли проверку через первоисточник. Так чрезвычайно важно заранее прорабатывать инструменты, не позволяющее обхитрить командующее звено армии.

Спутниковые снимки могут обеспечить высокоточное нанесение ударов по важным стратегическим пунктам противника, что осложнит его логистику и лишит возможности подвозить снаряжение для наступательных операций. Сегодня силовые структуры должны соответствовать критериям времени и активно использовать все возможные цифровые инструменты для сохранения жизни личного состава и повышения эффективности ведения как наступательных, так и оборонительных действий, а также проводить специальные образовательные программы среди сотрудников для успешного введения информационно-психологических спецопераций.

Список источников и литературы:

1. Ксения Демидкина. Аудитория русскоязычных каналов в Telegram выросла вдвое за 2022 год // Forbes. 20.01.2023 URL: https://www.forbes.ru/svoi-biznes/483954-auditoria-russkoazycnyh-kanalov-v-telegram-vyrosla-vdvoe-za-2022-god

2. Словарь. OSINT // Skillfactory media. 24.03.2003. URL: https://blog.skillfactory.ru/glossary/osint/

3. ITSumma. Какой софт использует ЦРУ и АНБ для дата-майнинга // Хабр. 17.09.2021. URL: https://habr.com/ru/companies/itsumma/articles/578460/

Чуклина Элена Юрьевна
научный сотрудник ЮНЦ РАН
E-mail: die_sehnsucht@mail.ru

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ДЕСТРУКТИВНОЙ ИНФОРМАЦИИ В СЕТИ «ИНТЕРНЕТ»

Аннотация. *Статья посвящена проблемам противодействия распространению деструктивной информации в Интернет-пространстве. Отмечается, что российские компетентные органы опираются преимущественно на репрессивный подход к борьбе с опасной информацией, который имеет как преимущества, так и недостатки. Оптимальным вариантом представляется соблюдение баланса между «жесткими» и «мягкими» мерами нейтрализации деструктивной информации, что способно обеспечить информационную безопасность граждан и использовать зарубежные Интернет-ресурсы в интересах России.*

Ключевые слова: *деструктивная информация, Интернет, ЛОМы, блокировка, информационные войны, фэйки, манипуляция, вербальные правонарушения.*

Актуальность. Интернет-платформы, в том числе зарубежные, прочно укрепились в жизни российских граждан. По данным отчета Global Digital 2023: Russian Federation [12], более 88 % населения России являются пользователями сети «Интернет», из них 73% регулярно используют социальные медиа. В рейтинге причин использования Интернета на третьем месте находится поддержка связи с друзьями и семьей, на втором — стремление быть в курсе новостей и событий, на первом — поиск информации. Примечательно, что в рейтинге причин использования социальных медиа, которые являются платформами по размещению и обмену пользовательского контента, первое место занимает общение с друзьями и семьей, чтение информационного материала — на третьем месте, поиск контента (любого без конкретизации) — на четвертом. В топ-5 сайтов по посещаемости вошли поисковики Google и Yandex, видеохостинг Youtube, социальная сеть

Вконтакте и Интернет-портал Mail.ru. В числе социальных сетей и мессенджеров у россиян в возрасте от 16 до 64 лет наиболее популярны ВКонтакте (75,3%) и принадлежащий признанной в России экстремистской организации Meta мессенджер Whatsapp (71,5%), от них немного отстает Telegram (64,4%), Одноклассники (43,5%) и TikTok (42,6%) занимают промежуточное место. Заблокированные в России социальные сети располагаются в самом конце рейтинга (не более 7%) вместе с малоизвестными iMessage и Likee, за исключением запрещенной в России социальной сети Instagram, которая по сравнению с 2021 г. потеряла порядка 37% пользователей, но все еще имеет 24% российской аудитории, получающей доступ через VPN-приложения и прокси-серверы.

Возраст пользователей социальных медиа отмечен неслучайно: официально в TikTok регистрироваться разрешено с 13 лет, в ВКонтакте — с 14 лет, в Likee — с 16 лет. Однако из-за отсутствия механизма аутентификации, позволяющего убедиться в возрасте нового пользователя, на перечисленных выше платформах аккаунты регистрируют дети и подростки любого возраста, имеющие доступ к Интернету. Например, администрация TikTok в 2021 г. удалила более 7 млн учетных записей, предположительно принадлежащих детям младше 13 лет [10]. В Likee, судя по контенту, владельцами аккаунтов являются преимущественно малолетние дети.

Вместе с тем перечисленные ресурсы содержат множество вредоносного контента. Е.И. Галяшина и В.Д. Никишин выделяют контентные и коммуникационные риски в качестве форм репрезентации девиантного речевого поведения в цифровой среде, к которым относятся пропаганда насилия и самоубийств, антиконституционных экстремистских идей, фейк-ньюс, открытая и скрытная вербовка в радикальные и деструктивные сообщества и т.д. [1]. С 2022 г. в сети «Интернет» заметно увеличилось число экстремистских высказываний в отношении россиян, призывы к террористическим актам и диверсиям на территории России, фейки об

исторических и текущих событиях, намеренное искажение информации в целях манипуляции общественным мнением.

Исследовательская проблема. Представители власти и эксперты испытывают трудности при разработке мер противодействия перечисленному деструктивному контенту, распространяемому в сети «Интернет», что ярко продемонстрировали дискуссии на XII Форуме безопасного Интернета [11]. Если представители законодательных и исполнительных органов склоняются к блокировкам, в частности, видеохостинга Youtube и электронной пользовательской энциклопедии Wikipedia, то среди экспертов чаще звучат призывы научиться говорить на одном языке с молодежью в Интернет-пространстве и использовать лидеров общественного мнения (далее – ЛОМы) для продвижения патриотической повестки, в том числе на зарубежных ресурсах. На текущий момент доминирует «жесткий» подход к противодействию деструктивной информации в Интернете. Согласно Постановлению Правительства РФ от 26.10.2012 № 1101 допускается блокировка сайтов не только по решению суда, но и исключительно по инициативе уполномоченных органов исполнительной власти. Так, за I квартал 2022 г. Роскомнадзором удалено 38 478 материалов, распространяемых в сети «Интернет», заблокировано 47 523 Интернет-ресурсов [6]. Действующее законодательство предусматривает ответственность за злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ) и так называемые вербальные преступления (ст. 207.1—207.3 УК РФ, публичные призывы к совершению преступлений, пропаганда и оправдание терроризма), совершение ряда преступлений с использованием информационно-коммуникационных технологий, включая сеть «Интернет», влечет более суровое наказание.

В этой связи курс на блокировку зарубежных Интернет-платформ выглядит реалистичным. С одной стороны, данное решение наиболее простое и эффективное с точки зрения закрытия доступа к деструктивной информации. На Youtube размещено множество видео с антироссийской риторикой и

дезинформацией относительно политических событий и экономической ситуации в стране, а российские каналы с большой аудиторией, напротив, получают перманентную блокировку. Wikipedia представляет Россию исключительно как агрессора в блоке информации о вооруженном конфликте с Украиной и не позволяет вносить изменения. С другой стороны, данная мера может вызвать недовольство населения, т.к. российские граждане интересуются в основном развлекательным, но не политическим контентом. Так, в 2022 г. россияне чаще всего смотрели на YouTube видео категорий «Музыка», «Развлечения», «Детский контент» и «Видеоигры» [5]. В трендах российского YouTube обычно располагаются музыкальные клипы и юмористические видео. По данным MEDIASCOPE, исходя из структуры запросов, видеохостинг остается преимущественно развлекательной площадкой [4]. В топ-50 популярных российских YouTube-каналов не входит ни одного политического блога [13]. При этом достойная альтернатива зарубежным ресурсам и, в частности, видеохостинг Rutube и Интернет-платформа Знание, пока не востребованы, поскольку нуждаются в доработке.

Кроме того, в силу закона сохранения материи, деструктивный контент с заблокированных ресурсов перетечет на доступные. Поэтому следующим шагом будет запрет оставшихся неотечественных Интернет-платформ, однако ВКонтакте даже сейчас не справляется с большим объемом опасной информации. Многие граждане продолжат использовать VPN и прокси.

Обзор литературы демонстрирует, что большинство трудов, посвященных деструктивному информационному воздействию в Интернете, принадлежат политологам, поскольку намеренное искажение информации и вбросы фейков – это политические технологии манипулирования массовым сознанием (С.В. Володенков, В.Б. Строганов и др.) [2; 9]. Важные результаты исследований по данной проблеме также встречаются в сфере юриспруденции, педагогики, психологии и философии (А.М. Столяренко, В.В. Вахнина, Е.А. Жукова и др.) [3; 8].

Однако и указанные специалисты испытывают трудности при рекомендации мер противодействия деструктивному информационному воздействию, что обусловлено, прежде всего, их «оторванностью» от популярных у молодежи Интернет-ресурсов. Выработке мер должен предшествовать длительный мониторинг ресурсов, осуществляемый лицом, которое является не только ученым или экспертом, но и активным пользователем Интернета, понимающим своеобразный Интернет-язык во избежание неправильной интерпретации контента.

При этом нерационально возлагать разработку инициатив по рассматриваемой проблеме на Совет блогеров, который будет защищать, прежде всего, собственные интересы. Так, например, предложение Совета блогеров о добровольной регистрации блогов в качестве СМИ [7] не имеет смысла, т.к. издержки (юридическая ответственность за контент) превышают выгоду (права журналистов, например, запросы в государственные органы и организации, аккредитация на общественно значимые мероприятия). Соответственно популярные блогеры проигнорируют данную возможность во избежание дополнительных ограничений: в развлекательной сфере возможности журналиста не востребованы, а политические инфлюенсеры привлекают аудиторию именно тем, что транслируют свое личное мнение (как бы близкое к народу) в качестве противовеса государственным СМИ.

Обязательная регистрация блогов в качестве СМИ внесла бы заметные изменения в деятельность инфлюенсеров и предлагаемый ими контент. Однако такая инициатива ставит множество вопросов: 1) Любой ли блог будет отвечать критериям СМИ, например, если контент состоит в зачитывании и комментировании новостей? 2) Будет ли аналогичная обязанность возложена на стримеров? 3) Как регулировать деятельность инфлюенсеров, находящихся за границей? и др.

На текущий момент функционирует несколько механизмов противодействия деструктивному информационному воздействию в Интернете: 1) блокировка сайтов и удаление материалов Роскомнадзором; 2)

модерация и использование нейросети в социальных сетях; 3) жалобы пользователей на запрещенный контент; 4) удаление информации по требованию органов власти; 5) признание иностранным агентом.

Из перечисленных методов самыми действенными являются первый и четвертый, однако они эффективны точечно. Поток запрещенного контента в социальных сетях, особенно в комментариях к постам сложно отследить и обработать. Контент-анализ ВКонтакте, в частности, новостного сообщества «Лентач» (2,4 млн подписчиков) и городского паблика «Ростов Главный — новости Ростова-на-Дону» (679 тыс. подписчиков), показывает, что модерация даже при поддержке нейросети пропускает в комментариях экстремистские высказывания, фейки и иной запрещенный контент.

Более того, закрытые группы ВКонтакте недоступны модераторам, что позволяет размещать любую опасную информацию для подписчиков группы до того момента, пока ими не заинтересуется ФСБ. Большинство пользователей не считают необходимым жаловаться на «язык вражды» или иной запрещенный контент, хотя это наиболее доступный и эффективный способ устранения вредной информации. Так, достаточно высокую результативность гражданской инициативы доказывает проект ОСПА российского блогера Стаса Васильева: массовая и организованная отправка жалоб администрации онлайн-платформы на экстремистские высказывания в адрес россиян и этнических русских, в результате чего автор запрещенного контента получает временную или постоянную блокировку. Данный метод работает даже на таких зарубежных ресурсах, как Youtube и Twitch, что, к сожалению, не отменяет блокировку пророссийских инфлюенсеров за их позицию, а не нарушение конкретных правил платформы.

Поэтому привлечение граждан к мониторингу и устранению деструктивной информации в сети «Интернет» выглядит перспективным способом, если это будет происходить в рамках организованного сообщества по типу ОСПА либо при взаимодействии граждан с Роскомнадзором (через

приложение РКН) или администрацией отечественных Интернет-ресурсов (через функцию «пожаловаться»).

Относительно придания статуса иноагента следует сказать, что данная мера действенна в случае нахождения источника деструктивной информации на территории России. Релоцировавшиеся инфлюенсеры превратили данный статус в имиджевое преимущество, утверждая, что это своеобразный знак качества, свидетельствующий о якобы правильности их позиции.

Заключение. В целом проблема деструктивного информационного воздействия требует изучения с различных ракурсов. Во-первых, следует выяснить, какой контент и Интернет-платформы предпочитают граждане разных возрастных категорий. Во-вторых, важен перманентный контент-анализ популярных отечественных и зарубежных ресурсов в соответствии с поставленными задачами (установить тренды, изучить манипулятивные технологии либо зафиксировать их отсутствие, оценить перспективы разблокировки некоторых ресурсов, например, Twitter ввиду новой политики Илона Маска). В-третьих, рекомендуется взглянуть иначе на феномен клипового мышления и мемов — с негативного восприятия переключиться на их потенциал в качестве инструментов пропаганды в положительном ключе (пропаганды здорового образа жизни, патриотизма). Наконец, в правовой регламентации деятельности в Интернете необходимо обеспечить баланс ограничений и свобод, чтобы не сложилась ситуация, когда инфлюенсеры и их аудитория будут вынуждены искать варианты обхода государственного надзора.

Список источников и литературы:

1. Галяшина Е.И., Никишин В.Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lex Russica. 2021. Т. 74. № 6 (175). С. 79-94;

2. Володенков С.В., Федорченко С.Н., Печенкин Н.М. Особенности формирования мировоззрения в условиях современной цифровой среды: анализ академических дискурсов // Дискурс-Пи. 2023. Т. 20. № 1. С. 8-26;

3. Жукова Е.А. Человек в плену Hi-Hume // Вестник ТГПУ. 2007. Вып. 11 (74). Серия: Гуманитарные науки (Философия). С. 29-35;

4. Медиа 2022: главные тренды. URL: https://mediascope.net/upload/iblock/1f6/8ha9kkrstxq4eed12mn3p8s6k5sglgnn/Медиа%202022%20День%20Бренда%20Ксения%20Ачкасова.pdf (дата обращения: 22.06.2023);

5. Музыка и развлечения: что искали россияне на YouTube. Инфографика. URL: https://www.rbc.ru/technology_and_media/14/11/2022/636e3ded9a794708e62556aa (дата обращения: 22.06.2023);

6. Результаты деятельности Роскомнадзора за 1 квартал 2022 года. URL: https://rkn.gov.ru/plan-and-reports/reports/p449/ (дата обращения: 28.05.2023);

7. Совет блогеров выступил в Госдуме с предложением ввести добровольную регистрацию блогов как СМИ. URL: https://sovet-blogerov.ru/23-12-22 (дата обращения: 29.05.2023);

8. Столяренко А.М., Сердюк Н.В., Вахнина В.В., Боева О.М., Грищенко Л.Л. Психологические аспекты деструктивного информационно-психологического воздействия // Психология и право. 2019. Том 9. № 4. С. 75-89;

9. Строганов В.Б. Технологии политической манипуляции в Интернете: дис. … к.п.н.: 23.00.02. Екатеринбург, 2020. 209 с.;

10. Терешин А. TikTok удалил миллионы аккаунты детей. URL: https://secretmag.ru/news/tiktok-udalil-milliony-akkauntov-detei.htm (дата обращения: 28.05.2023);

11. XII Форум безопасного Интернета 2023 — Лига безопасного Интернета. URL: https://ligainternet.ru/forum-bezopasnogo-interneta/ (дата обращения: 28.05.2023);

12. Digital 2023: The Russian Federation – DataReportal — Global Digital Insights. URL: https://datareportal.com/reports/digital-2023-russian-federation (дата обращения: 28.05.2023);

13. Top 100 YouTubers in Russian Federation sorted by SB rank. URL: https://socialblade.com/youtube/top/country/ru (дата обращения: 22.06.2023).

СЕКЦИЯ 3

«ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СОВРЕМЕННЫЕ МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ»

Брачунова Алиса Валерьевна
бакалавр кафедры всеобщей истории, международных отношений
и документоведения
Самарский национальный исследовательский университет
имени академика С.П. Королева
E-mail: alisabrachunova@gmail.com

КОНФЛИКТ В ЮЖНО-КИТАЙСКОМ МОРЕ КАК ПРИЧИНА ВОЗНИКНОВЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСЕАН, КИТАЯ И США

Аннотация. *Спор в Южно-Китайском море является одним из очагов конфликта, который уже давно вышел за рамки региона и сейчас постепенно перерастает в глобальный формат/уровень. Актуальность исследования обусловлена развитием конфликта в худшую сторону, в частности в информационных пространствах стран. Однако информационной стороне конфликта практически не уделяется внимания в научном сообществе, но с каждым годом цифровая среда всё больше укореняется в жизни государств, особенно как инструмент политического влияния. Именно поэтому возникает необходимость изучить конфликт в Южно-Китайском море в информационном пространстве. В статье рассмотрены основные столкновения стран АСЕАН, Китая и США в цифровом пространстве, выявлены практические рекомендации для смягчения конфликта.*

Ключевые слова: *Южно-Китайское море, АСЕАН, информационная безопасность, кибератаки, Китай, США.*

Введение. Сегодня конфликт в Южно-Китайском море (далее – ЮКМ) является одним из наиболее острых вопросов международных отношений. Его также называют «пороховой бочкой Азии». От путей его разрешения и исхода зависят экономические перспективы большого количества государств и организаций, а именно АСЕАН, включая Бруней, Вьетнам, Тайвань (частично признанное государство), Малайзию, Филиппины и Китайскую Народную Республику. Можно полагать, что в зависимости от исхода конфликта, будет провозглашён не только региональный лидер, но и изменён глобальный

порядок. Всё более активно начинает проявлять себя США и их союзники (Quad group of nations – QUAD), так как Южно-Китайское море представляет очаг напряжённости, способный поменять современный уклад международных отношений. Ключевыми факторами для продолжения конфликта являются несогласованность границ экономических зон, морских научных исследований, рыбного промысла, а также споры по поводу принадлежности морского шельфа, Парасельских островов, островов Спратли.

История противостояния в информационном пространстве. Хотя гибридная война может представляться довольно избитой концепцией, новым ключевым элементом этой «мягкой войны» являются цифровая среда и информационная безопасность. Действия на «цифровых» полях сражений для стран-участниц конфликта ЮКМ начались ещё в 2010-х годах. Первая крупная кампания против Филиппин в связи с территориальным спором произошла в апреле 2012 года после напряженного противостояния между китайскими и филиппинскими судами на принадлежащей Филиппинам отмели Скарборо. Китайское подразделение взломало правительственные и военные сети в островном государстве, похитив военные документы и другие конфиденциальные сообщения, связанные с конфликтом.

В 2015 году в то время, как другие страны были возмущены претензиями компартии Китая (КПК) на спорные территории в Южно-Китайском море, назрел ещё один конфликт. Хакерская группа Anonymous начала новую операцию, чтобы противостоять захвату территорий китайским режимом в Южно-Китайском море. Они назвали операцию #OpStopReclamation. В Twitter информация по операции находилась на страничке #OpChina, которая ранее использовалась для поддержки прав человека в Тибете и демократических протестов в Гонконге. В рамках операции Anonymous взломали 7 китайских правительственных сайтов, 10 образовательных и 64 коммерческих веб-сайта. Атаки якобы совершили члены Anonymous на Филиппинах. На каждом взломанном сайте они оставили сообщение: «Многие из вас знают о

деспотичных действиях правительства Китая в Южно-Китайском море… Их претензии в указанном районе — не что иное, как просто предположения, не имеющие твёрдых доказательств» [1].

В 2016 году вердикт Гаагского Третейского суда, признавшего юридическую несостоятельность претензий Пекина на единоличный контроль над островами в Южно-Китайском море, был широко поддержан правительствами и общественностью США, Японии и Филиппин. Во Вьетнаме также с одобрением отнеслись к решению суда, но подчеркнули, что выступают исключительно за мирное решение территориальных споров. После этого хакеры группы 1937CN на несколько минут сумели заблокировать системы оповещения в международных аэропортах Ханоя и Хошимина и запустить на мониторах видеоролики со своей символикой и заявлением, что эти острова принадлежат КНР. Одновременно по системе звукового оповещения звучал мужской голос, который на английском языке критиковал позицию вьетнамских властей по спорным островам. Затем был взломан Интернет-сайт авиакомпании Vietnam Airlines, национального авиаперевозчика Вьетнама, и на его главную страницу было выведено то же изображение [2, с.42-48]. Правительство СРВ было озабочено нападениями хакеров, которые наносили существенный экономический ущерб, а также угрожали имиджу и политическому строю страны. Одновременно с этим, сообщает издание VNExpress, Вьетнам сам является крупным источником кибератак [3]. Так, в четвертом квартале 2018 г. вьетнамские хакеры совершили 992 952 атаки. Невозможно вычислить, сколько из них было направлено на Китай или другие страны АСЕАН. Вообще установить конкретных авторов кибератак, если они не хотят себя раскрывать, довольно сложно, что значительно затрудняет решение конфликтов в сфере информационной безопасности. Примерно в то же время кибератаки коснулись и Филиппин: по меньшей мере 68 веб-сайтов национальных и местных органов власти на Филиппинах были отключены в результате массовой распределенной атаки типа «отказ в обслуживании» (DDoS).

В 2018 году китайская группа, получившая название TEMP.Periscope, искала информацию, которая может принести пользу китайскому правительству, сообщила компания FireEye, поставщик сетевых систем защиты из США. Хакеры сосредоточились на морских организациях США, которые либо были связаны с Южно-Китайским морем, либо клиентами, работающими в акватории. Данные, полученные в ходе инцидентов, могли быть использованы, например, для определения того, насколько близко судно может плыть к географическому объекту. «Это определенно тот случай, когда они могут использовать информацию для принятия стратегических решений» - прокомментировала компания [4]. Интересно, что данная хакерская организация также обвинялась в шпионаже в Камбодже.

Примечательно, что Китай не страдает от атак, имея защиту своего информационного пространства. Принимая во внимание все риски и возможности, КНР создает благоприятный информационный климат внутри страны и не дает воздействовать на него извне, в частности, тщательно фильтруются любые статьи и высказывания по поводу Южно-Китайского моря [5, с.382–394].

Заключение. Таким образом, можно сделать выводы о непрекращающемся информационном аспекте конфликта и сформулировать практические рекомендации:

1. Существует необходимость внесения пункта об информационной безопасности всех сторон конфликта в разрабатывающийся Кодекс поведения сторон в Южно-Китайском море (COC);

2. Следует разработать соглашения между США и Китаем по информационной безопасности в регионе АТР, как главных противоборствующих сторон в регионе;

3. Требуется отказ от взаимных атак в цифровом пространстве, меры по сотрудничеству и консолидации в вопросах информационной между АСЕАН и Китаем, подкреплённые соглашениями при международных наблюдателях-посредниках.

Список источников и литературы:

1. Джошуа Ф. Конфликт в Южно-Китайском море спровоцировал битву между хакерами // THE EPOCH TIMES, 2 июня 2015 г. [Электронный ресурс] URL: https://www.epochtimes.ru/konflikt-v-yuzhno-kitajskom-more-sprovotsiroval-bitvu-mezhdu-hakerami-98985893/ (дата обращения: 14.05.2023)

2. Довгий С., Колотов В., Сторожук Н. Влияние кибербезопасности на суверенитет страны и перспективы Российско-Вьетнамского сотрудничества // Первая миля. 2019. № 6 (83).

3. Число кибератак на Вьетнам уступает лишь числу кибератак на Россию // Регнум, 25 января 2019 г. [Электронный ресурс] URL: https://regnum.ru/news/2559489 (дата обращения: 14.05.2023)

4. Tweed D. Chinese Hackers Hit U.S. Firms Linked to South China Sea Dispute // Bloomberg, 16 March 2018. [Электронный ресурс] URL: https://www.bloomberg.com/news/articles/2018-03-16/china-hackers-hit-u-s-firms-linked-to-sea-dispute-fireeye-says (дата обращения: 14.05.2023)

5. Понка Т. И., Рамич М. С., Ву Ю. Информационная политика и информационная безопасность КНР: разработка, подходы и реализация // Вестник РУДН. Международные отношения. 2020. № 2 (20).

6. Васильев Д., Шавлай Э. Южно-Китайское море в противостоянии КНР И США в Азии // Азия И Африка Сегодня. [Электронный ресурс] URL: https://mgimo.ru/upload/iblock/7c1/Azia-07-2020_61-66-min.pdf (дата обращения: 14.05.2023)

7. Мосяков Д.В., Астафьева Е.М. Ситуация в Южно-Китайском море после вердикта международного арбитражного суда в Гааге // ЮГО-ВОСТОЧНАЯ АЗИЯ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ. URL: file:///C:/Users/User/Downloads/situatsiya-v-yuzhno-kitayskom-more-posle-verdikta-mezhdunarodnogo-arbitrazhnogo-suda-v-gaage%20(1).pdf (дата обращения: 14.05.2023)

8. Saalman L. New domains of crossover and concern in cyberspace // SIPRI, 26 July 2017. [Электронный ресурс] URL:

https://www.sipri.org/commentary/topical-backgrounder/2017/new-domains-crossover-and-concern-cyberspace (дата обращения: 14.05.2023).

Гаврилова Анастасия Сергеевна
студент 2 курса кафедры международных отношений
Санкт-петербургский государственный экономический университет
E-mail: AnastasiaGavrilova-1@yandex.ru

Марков Александр Анатольевич
заведующий кафедрой международных отношений
Санкт-петербургский государственный экономический университет
E-mail: mark08@list.ru

ИНФОРМАЦИОННАЯ ВОЙНА КАК ФАКТОР УГРОЗЫ ДЛЯ СОВРЕМЕННОЙ СИСТЕМЫ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Аннотация. *Повышение интеллектуального уровня человечества послужило естественным толчком к развитию глобальной научно-технической мысли, появлению новых видов компьютерных технологий и усовершенствованию уже имеющихся. Бурное развитие информационно-коммуникационных технологий (ИКТ) предопределило начало новой информационно-технологической эры. Концепция цифрового века включает в себя массовое внедрение ИКТ во все сферы жизни общества и интенсификацию информационных потоков. На сегодняшний день межгосударственные отношения характеризуются усилением конкуренции, которая, в свою очередь, требует использование новых средств и методов воплощения национальных интересов. В то же время повышение градуса политической напряжённости на мировой арене сопровождается постепенным отказом государств от силового воздействия на противника. Исторический опыт показал, что способность оказывать влияние, в том числе и информационное, на глобальные международные процессы может быть более важной, чем обладание значительным военным потенциалом или экономическим могуществом; а применение «традиционной» силы не ведет автоматически к мировой гегемонии. В этих условиях возникли новые, специфичные именно для информационной эпохи угрозы и, как следствие, новые формы ведения боевых действий. В данной статье рассматривается*

феномен информационной борьбы в качестве важного средства защиты национальных интересов государства.

Ключевые слова: *информационное противоборство, международные отношения, глобализация, информация*

Введение. Во все времена информация являлась необходимым для выживания инструментом познания мира и коммуникации с ним. Эволюционное развитие человека сопровождалось накоплением, обобщением и углублением сведений об окружающем мире. На основе полученных и систематизированных знаний человечество переходило с одной ступени развития на другую. В процессе этногенеза люди научились использовать информацию не только в качестве орудия созидания и познания, но и в качестве мощной разрушительной силы.

Феномен информационной войны в современном мире. Формы информационного влияния постепенно менялись вместе с типами общества. Переход к постиндустриальному обществу был определён стремительным развитием ИКТ и их дальнейшим внедрением во все сферы деятельности человека. В свою очередь, это привело не только к кардинальной трансформации технологических укладов, но и к формированию глобальной информационной среды, которая изменила характер взаимоотношений между государствами.

«Кто владеет информацией, тот владеет миром» □ знаменитая фраза Натана Ротшильда, которая не только не теряет своей актуальности на протяжении многих веков, но и всё чаще используется для описания состояния современных международных отношений[4]. Непрерывно формирующееся глобальное информационное пространство постепенно стирает границы между государствами, что значительно расширяет поле борьбы между ними. Кроме того, создаются благоприятные возможности активного вмешательства одного государства во внутренние дела своих противников.

Наступление технологической эры привело и к модификации форм геополитического противоборства. Внедрение информационных технологий

во все структуры жизнеобеспечения государства; снижение цен на компьютерные системы и их продукты в связи с широким распространением ИКТ, уязвимости в архитектуре различных компьютерных сетей, а также отсутствие единой межгосударственной системы правового регулирования инфосферы увеличили возможность прямого доступа к ресурсам компьютерной системы государства-противника из любой точки земного шара[3]. В связи с этим на сегодняшний день всё четче обозначается тенденция использования информации в качестве основного средства оказания влияния на потенциального противника во взаимодействии между субъектами международного сообщества. Указанные причины послужили толчком развития информационной войны в качестве новой формы современных социально-политических конфликтов.

Термин «информационная война» появился в лишь в середине 80-х годов XX столетия в результате генезиса научного знания. Данная специфическая форма международной коммуникации ещё не имеет понятийной устойчивости: существует множество подходов изучения информационной войны, что свидетельствует об отсутствии единой точки зрения относительно сущности, целей и задач, субъектов и объектов, методов и средств ведения и т.д. На разных этапах развития человечества информация претерпевала различные трансформации своей роли в обществе, наиболее значительная из которых произошла в середине прошлого века. В современной исследовательской среде наблюдается рост интереса к изучению информации как основного инструмента современной глобальной политики. Выходя на качественно новый уровень, информация становится неотъемлемым структурным элементом всех сфер жизни общества и отражает мощь, прогрессивность и благополучие любого государства [1, с.23].

С развитием человечества трансформировались и формы информационной борьбы: произошёл переход от простейшего вида воздействия к сложно организованному с применением всех доступных коммуникационных каналов. Характерной чертой современной

информационной борьбы является её комбинированный характер, который определяется использование новых, модифицированных методов поражения противника в традиционных сферах жизнедеятельности общества.

Современное информационное противоборство определяется и следующими особенностями [1, с. 32-35]:

1. Использование информационного пространства в качестве поля противоборства между акторами международных отношений.
2. Отсутствие четких границ между государствами в информационном поле позволяет оказывать информационное воздействие на все сферы общественной жизни.
3. Информационное давление на соперника осуществляется постоянно и непрерывно [4].
4. Информационное противоборство может иметь как латентную, так и открытую стадию.
5. Для информационной борьбы используется всё многообразие коммуникационных каналов.
6. Противоборствующие стороны могут вносить коррективы в реальном времени.

В результате длительного генезиса была сформирована структура ведения информационной борьбы, которая включает в себя цели и набор инструментов, необходимых для их достижения.

Информационно-сетевое противоборство предполагает проведение комплекса мероприятий с целями [1, с.65-79]:

1. Сбора, искажения, хищения и/ или уничтожения особо важной для государства-противника информации.
2. Полного изменения культурной сферы страны-оппонента путём навязывания чуждых ему идеалов и ценностей, что создает благоприятную атмосферу для возникновения конфликтной обстановки.

3. Явного или косвенного вмешательства в политический процесс государства путём воздействия на политические элиты для изменения типа управления, подмены целей государственного курса [3].

4. Нарушения внутреннего порядка с помощью привлечения к участию в несанкционированных публичных мероприятиях, направленных на дестабилизации общественно-политической обстановки государства поражения, подрыва авторитета власти, утраты доверия.

Для достижения поставленных целей используются различные виды информационного оружия, которые способны усилить эффект от информационного воздействия на государство-противника.

В настоящее время ключевым условием безопасности любого государства является правильное использование имеющейся информации. Информационный фактор используется как инструмент для оказания различного рода влияния на систему современных международных отношений. В условиях новой реальности борьба за выгодное положение в мире и возможность реализовать свои национальные интересы сопровождается непрерывным информационным воздействием на оппонентов. Ярким примером этих тезисов являются отношения между Россией и Украиной и их союзниками.

Начиная с первого десятилетия этого столетия, отношения между этими субъектами имеют конфликтный потенциал в различных областях. В свою очередь, стремительное развитие и широкое распространение информационных технологий привело к превращению информации в наиболее ценную стратегическую, предопределило борьбу за право обладать ею и оправдало перенос борьбы между двумя державами в информационное поле. С 2014 года вся деятельность Украины и западных стран сопровождается мощным и согласованным информационным воздействием, которое постепенно принимает форму информационной борьбы [2].

Любые изменения в общественно-политической сфере являются поводом для начала информационной борьбы. Например, воссоединение

Крыма с Российской Федерацией в результате референдума в 2014 году стало крупнейшей геополитической перестановкой в системе международных отношений. В связи с этим случаем Украина взяла курс на полный разрыв экономических, культурных и политических связей с Россией.

На протяжении длительного периода времени наше государство является главным объектом непрекращающейся информационного воздействия со стороны Украины и её западных партнёров, которое проводится через глобальное информационное поле. В связи с этим сегодня для Российской Федерации на первый план выходит вопрос защиты своих национальных интересов в инфосфере. Для обеспечения информационной безопасности РФ и сохранения её статуса крупнейшего глобального игрока важно не только организовать грамотный ответ на информационно-сетевое воздействие, но и реализовывать политику в информационной среде в соответствии с потребностями современного развития глобального информационного общества.

Как в 2014, так и в 2022 г. Российская Федерация осуществляет своё информационное воздействие на иных субъектов международного общения на основе принципов объективного изложения случившегося и организации открытого равноправного диалога между различными информационных агрегаторами.

В условиях эскалации российско-украинского конфликта в 2022 году информационная война стала продолжением стратегии ослабления позиций России на мировой арене, которая уже несколько лет реализуется Украиной при поддержке Запада. В связи с этим способность нашего государства противостоять агрессивной риторике является приоритетной задачей обеспечения национальной безопасности [2]. Очевидно, что в условиях беспрецедентного информационного давления Россия нуждается в единой информационной политике, организации пропаганды и контрпропаганды, а также в создании советующих структур, в том числе и для деятельности за рубежом.

Заключение. Таким образом, стремительно набирающая обороты глобальная информатизация общества диктует свои требования. Дальнейшее развитие и распространение ИКТ позволит информационному противоборству стать самостоятельной формой геополитического противостояния. В связи с этим в условиях повышения значимости информационного ресурса сильное государство – это государство, не только обладающее значительным военным и экономическим потенциалом, но и умеющее отстаивать свои национальные интересы путём успешного информационного воздействия на своих оппонентов. Обеспечение информационной безопасности является предметом интересов акторов современной системы международных отношений на данном этапе своего развития. Изучение истоков информационной борьбы, а также её структуры и методов, а также формировании стратегии информационной борьбы позволит успешно противостоять информационному давлению со стороны геополитических соперников и минимизировать его негативные последствия.

Список источников и литературы:

1. Воронова О. Е. Современные информационные войны: типология и технологии / О.Е. Воронова — Рязань, 2018. — 188 с.

2. Мальчикова В. Информационное пространство Украины в контексте противостояния Запада и России/ В. Мальчикова – 2018. [Электронный ресурс]. – Режим доступа: https://nic-pnb.ru/politicheskij-krizis-na-ukraine/informatsionnoe-prostranstvo-ukrainy-v-kontekste-protivostoyaniya-zapada-i-rossii/ (дата обращения: 18.04.2023).

3. Степанова Н. С. Информационное противоборство на современном этапе: анализ и тенденции / Н. С. Степанова. // Молодой ученый. — 2009. — № 2 (2). — С. 252-256. [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/2/153/ (дата обращения: 17.04.2023).

4. Удовик В.Е. Информационная революция и становление информационного общества / В.Е. Удовик, А.В. Селютин- 2015. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnaya-

revolyutsiya-i-stanovlenie-informatsionnogo-obschestva/viewer (дата обращения: 18.04.2023).

Иванов Евгений Олегович
редактор Интернет-вещания телеканала RT на испанском языке
E-mail: eugene4712@mail.ru

БРАЗИЛИЯ: ЭВОЛЮЦИЯ ПОДХОДОВ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПУТИ К «ЦИФРОВОМУ СУВЕРЕНИТЕТУ»

Аннотация. *Настоящая статья посвящена подходам Бразилии к международной информационной безопасности (МИБ). Будучи важной региональной державой с глобальными амбициями, Бразилия активно вовлечена в дискуссии по теме МИБ и её различным аспектам, участвуя в профильных международных форматах и разрабатывая доктринальные документы по данной теме. На основании изучения научной литературы и нормативно-правовой базы автор приходит к выводу, что подходы Бразилиа к МИБ основаны на уважении суверенитета, невмешательстве во внутренние дела и недопущении милитаризации ИКТ-среды.*

Ключевые слова: *Бразилия, международная информационная безопасность, Группа правительственных экспертов, управление Интернетом, милитаризация ИКТ, персональные данные, меры по укреплению доверия, угрозы МИБ.*

Внешняя политика Бразилии характеризуется стратегией «автономии через диверсификацию», основанной на трепетном отношении к суверенитету, стремлении к региональному лидерству и активном участии в структурах глобального управления, а также диверсификации внешних связей [1, с. 360-361]. Применительно МИБ это означает, что Бразилия руководствуется принципами уважения суверенитета, невмешательства во внутренние дела и добросовестного международного сотрудничества с целью выработки юридически обязательных международно-правовых норм в данной сфере.

Бразилия участвовала в Группе правительственных экспертов (далее – ГПЭ) с самого начала её работы в 2004 году. Тогда итоговый доклад не был принят в силу разногласий по предмету обсуждения. Они касались

использования ИКТ в военно-политических целях и негативного воздействия вредоносных информационных технологий на систему глобальной безопасности. Бразилия, наряду с Россией, Китаем, ЮАР, Малайзией, Белоруссией и Южной Кореей, отстаивала важность не только обсуждения этих угроз, но и выработки соответствующего документа по противодействию им на базе Первого комитета Генеральной Ассамблеи ООН, занимающегося проблемами разоружения и международной безопасности. В то же время США и их союзники предлагали обсуждать использование ИКТ только в террористических и преступных целях [6, с. 16].

Также Бразилия уделяет значительное внимание управлению Интернетом. Её подход основан на принципах Тунисской повестки, принятой по итогам Всемирного саммита по вопросам информационного общества 2005 года: международное управление Интернетом должно быть многосторонним, открытым и демократичным, в него должны быть вовлечены государства, частный сектор, гражданское общество и международные организации, и у каждого из акторов должны быть чётко прописаны права и обязанности в данной сфере. При этом для Бразилии важно, чтобы ни один актор не располагал полным господством в данной области. Кроме того, бразильское руководство активно обсуждает тему управления Интернетом на площадках МЕРКОСУР, ИБСА, БРИКС, G20 и ООН, уделяя последней особое внимание в сфере противодействия милитаризации ИКТ-среды и мирного разрешения споров в цифровой сфере [7, p. 57-58].

В апреле 2014 года в бразильском городе Сан-Паулу прошла Глобальная встреча с широким кругом участников по будущему Интернета (NETmundial), председателем которой выступил координатор Управляющего комитета Бразилии по обеспечению работы Интернета и секретарь по разработке политики в сфере ИКТ Министерства науки, технологии и инноваций Виргилио Фернандес Алмейда.

На мероприятии выступила и тогдашний президент Бразилии Дилма Руссефф, выступившая в поддержку «многосторонней модели» управления

Интернетом, где одинаково представлены как государственные, так и негосударственные акторы, в том числе частные компании, общественные организации, НКО, научное сообщество. Вместе с тем, именно государства, по её мнению, играют особую роль в защите прав человека, в том числе и в Интернете. Кроме того, Д.Руссефф выступила за нейтральность Интернета и против несанкционированного вмешательства в частную жизнь граждан, а также поддержала право на всеобщий доступ к сети [14].

Заявление, принятое по итогам форума, содержало большинство принципов, разделяемых Бразилией. Так, в итоговый документ вошло право на всеобщий доступ к Интернету и защиту персональных данных от несанкционированного вмешательства. Также констатирована необходимость многостороннего, открытого, равноправного, ответственного и основанного на сотрудничестве и консенсусе механизма управления Интернетом. По вопросу нейтральности сети было принято решение продолжить дискуссии [13].

В 2015 году председателем ГПЭ четвёртого созыва стал Карлос Луис Перес, начальник канцелярии замглавы МИД Бразилии по политическим вопросам. Принятый итоговый доклад конкретизировал меры по недопущению атак на объекты критической инфраструктуры, применения вредоносного программного обеспечения в производстве ИКТ и использования групп экстренного реагирования на компьютерные инциденты в осуществлении кибератак, а также атак против таких групп. Кроме того, доклад содержал разделяемые Бразилией установки по защите цифрового суверенитета государств, суверенному равенству в ИКТ-среде и невмешательству во внутренние дела других государств по вопросам ИКТ [2].

Камнем преткновения стал вопрос о применимости норма международного гуманитарного права к ИКТ-среде. Бразилия, наряду с Россией, Китаем, Индией и рядом других незападных государств, является членом Группы одиннадцати (G11), придерживающейся общей позиции по вопросу будущего МИБ, которая состоит в недопущении гонки

информационных вооружений и развязывания информационных и «кибервойн» [5, с. 284].

Говоря о внутреннем законодательстве Бразилии по вопросам обеспечения информационной безопасности, стоит, в первую очередь, отметить Белую книгу национальной обороны Бразилии от 2012 года. В соответствии с ней безопасность ИКТ считается одним из трёх стратегических секторов, наряду с ядерными и космическими технологиями. В рамках сухопутных войск Бразилии в 2010 году учреждён Центр по обороне в ИКТ-среде, в задачи которого входят защита от атак в ИКТ-среде, реагирование на компьютерные инциденты, укрепление потенциала «кибербезопасности» страны, рекомендации по обновлению доктринальных документов по вопросу безопасности ИКТ, а также подготовка кадров в данной сфере [12, p. 71-72]. Центр сыграл важную роль в предотвращении атак против инфраструктуры ИКТ в ходе Чемпионата мира по футболу в 2014 году и Олимпийских игр в Рио-де-Жанейро в 2016 году [3, с. 47].

В некотором роде поворотным моментом в подходах Бразилии к МИБ стал 2013 год. Тогда после разоблачений Эдварда Сноудена стало известно, что спецслужбы США осуществляли электронный шпионаж за главами ряда государств и их ближайшим окружением. Бразилия не осталась в стороне от подобных схем. Американские спецслужбы прослушивали и отслеживали переписку Д. Руссефф и её родственников, а также руководства силовых структур, МИД Бразилии и государственной нефтяной компании Petrobras.

Бразилия соответствующе отреагировала на подобное вмешательство во внутренние дела. Помимо высылки посла США Томаса Шелдона и приостановки ряда сделок в сфере военно-технического сотрудничества, было активизировано взаимодействие по вопросам МИБ на региональном уровне и в рамках БРИКС. Кроме того, в 2015 году был начат проект по прокладыванию Интернет-кабеля из Европы в Бразилию в обход США по дну Атлантического океана [4].

Скандал повлиял и на внутреннее законодательство Бразилии. В апреле 2014 года был принят закон №12.965, также известный как «Билль Марко» [11]. Закон уделял приоритетное внимание правам и свободам человека в информационном пространстве и безопасности личных данных, а также практическим мерам по их обеспечению. В частности, статья 7 «Билля Марко» закрепляла права всех граждан Бразилии на тайну и неприкосновенность личной переписки, за исключением случаев вынесения соответствующих судебных решений. Статья 11 закона предусматривала применимость его положений к юридическим лицам, штаб-квартира которых находится за пределами Бразилии. Статья 12, в свою очередь, обозначала санкции для нарушителей прав бразильских граждан в цифровом пространстве: предупреждение с обозначением крайнего срока для устранения нарушений, штраф вплоть до 10% от чистой прибыли нарушителя в Бразилии за последний финансовый год, временное или полное приостановление деятельности нарушителя на территории страны [11].

14 августа 2018 года на базе «Билля Марко» был принят Общий закон о защите персональных данных (Lei Geral de Proteção de Dados Pessoais, LGPD). Закон закреплял, что в основе защиты данных лежат принципы свободы и неприкосновенности частной жизни, свободы слова, мнений и информации, а также задачи экономического и технологического развития и обеспечения свободной конкуренции. Кроме того, предписывалось информировать субъекта персональных данных о целях их обработки: сбора, использования, хранения, передачи третьим лицам и другим операциям [10].

Для контроля за соблюдением LGPD учреждалось специальное ведомство – Национальный орган по защите данных (Autoridade Nacional de Proteção de Dados, ANPD), получивший широкие полномочия в данной сфере. Согласно статье 55 закона, ведомство должно заботиться о защите персональных данных, промышленной и коммерческой тайны; осуществлять нормативно-правовую работу в сфере защиты данных; анализировать национальную и международную практику по данному вопросу;

взаимодействовать с другими государственными структурами в области своей компетенции, сообщая им обо всех нарушениях LGPD, включая совершённые госструктурами; сотрудничать с ведомствами других государств, отвечающими за безопасность данных [10].

Также в 2018 году бразильское руководство приняло стратегию цифровой трансформации «Повестка дня для цифрового общества будущего» (далее – Стратегия-2018) [8]. Документ уделил внимание вопросам обеспечения МИБ и роли Бразилии в этих вопросах, а также обеспечению национальной безопасности страны в цифровой среде, предложив комплекс мер для успешной борьбы с угрозами информационной безопасности страны.

Во-первых, был создан Межведомственный комитет по цифровой трансформации (Comitê Interministerial para a Transformação Digital, CITDigital), куда вошли по три представителя из ряда подразделений офиса президента Бразилии (Управление институциональной безопасности, Генеральный секретариат и Гражданская палата), а также из МИД, Минэкономики, Минобразования, Министерства коммуникаций и Министерства науки, технологий и инноваций. На CITDigital были возложены следующие основные полномочия: согласование государственной политики в цифровой сфере со Стратегией-2018, взаимодействие с властями штатов и муниципалитетов и международное сотрудничество, а также совершенствование нормативно-правовой базы по данному вопросу [8].

Во-вторых, критическим моментом была признана подготовка кадров для обеспечения информационной безопасности государства с целью гарантировать технологическую автономию Бразилии, особенно в сфере технологий и информации двойного назначения, а также создание технической основы для успешной защиты критической инфраструктуры страны от атак в ИКТ-среде.

Наконец, Стратегия-2018 уделяла значительное внимание международным проблемам в сфере информационной безопасности. В частности, особо выделены вопросы укрепления лидерства Бразилии в рамках

международных форумов по вопросам МИБ, содействия региональной интеграции в цифровой экономике и повышения цифровой конкурентоспособности бразильских компаний, в том числе малого и среднего бизнеса за рубежом путём расширения электронной торговли [8].

Два года спустя вступила в силу Национальная стратегия Бразилии в области кибербезопасности (далее – Стратегия-2020) [9]. Документ выделил три основные цели Бразилии в обеспечении информационной безопасности: усиление возможностей страны в цифровом пространстве, повышение устойчивости к угрозам ИКТ и рост влияния Бразилиа в вопросе обеспечения МИБ на международной арене. Последняя цель включает в себя не только участие Бразилии в международных дискуссиях и форумах по МИБ, но и подписание новых соглашений о сотрудничестве в данной сфере, а также проведение соответствующих учений. Отдельным пунктом указана важность сотрудничества Бразилии с другими государствами Латинской Америки по актуальным проблемам МИБ, что подчёркивает её стремление к региональному лидерству в данном вопросе [9]. Стратегия-2020 также закрепила основные принципы, которыми руководствуется Бразилиа в рамках международного сотрудничества по МИБ: мультилатерализм, уважение прав человека, соблюдение международного права и мирное разрешение споров. Согласно документу, для безопасной цифровой средыв глобальном масштабе важны меры по укреплению доверия, нацеленные на межгосударственное сотрудничество и обмен информацией в области МИБ, открытость и предсказуемость, а также укрепление всеобщего мира и стабильности. Среди главных угроз МИБ выделены преступность и шпионаж в сфере использования ИКТ, атаки на критическую инфраструктуру, массовый перехват данных и наступательные операции с применением ИКТ для проецирования силы в мирное время [9].

Заключение. На основе проведенного исследования, можно констатировать, что в своей международной деятельности и основополагающих документах Бразилия последовательно отстаивает

стремление к лидерству в области МИБ. Её подходам присущи такие черты, как стремление к обеспечению цифрового суверенитета при одновременной открытости для добросовестного и равноправного сотрудничества на двустороннем, региональном и глобальном уровнях, невмешательство во внутренние дела, а также артикуляция угроз МИБ как негосударственного, так и государственного характера.

Список источников и литературы:

1. Борзова А.Ю. Бразильская концепция «Автономии» как основа внешнеполитической стратегии страны // Актуальные проблемы международных отношений и внешней политики в XXI веке: монография / под ред. Т.В. Кашириной и В.А. Аваткова. – 3-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2019. – С. 347-369.

2. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, 22 июля 2015 года // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 26.04.2023).

3. Макарычева А.В. Информационная безопасность в Латинской Америке: пути адаптации к новым угрозам // Латинская Америка. – 2018. – №1. – С. 45-53.

4. Манойло А.В. Страны БРИКС на пороге создания собственной киберполиции // Экспертный институт социальных исследований. URL: https://eisr.ru/news-and-announcements/strany-briks-na-poroge-sozdaniya-sobstvennoy-kiberpolitsii/ (дата обращения: 26.04.2023).

5. Международная информационная безопасность: Теория и практика. Т.1: учебник для вузов / Под общ. ред. А.В. Крутских. – М.: Издательство «Аспект Пресс», 2021. – 384 с.

6. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. – А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с.

7. Brazilian Digital Transformation Strategy: E-Digital. Brasília, 2018. 115 p.

8. Estratégia Brasileira para a Transformação Digital, de 21 de março de 2018 // Presidência da República. URL: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9319.htm (дата обращения: 26.04.2023).

9. Estratégia Nacional de Segurança Cibernética, de 5 de fevereiro de 2020 // Presidência da República. URL: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Decreto/D10222.htm (дата обращения: 26.04.2023).

10. Lei Geral de Proteção de Dados Pessoais, de 14 de agosto de 2018 // Presidência da República. URL: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (дата обращения: 26.04.2023).

11. Lei №12.965, de 23 de abril de 2014 // Presidência da República. URL: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm (дата обращения: 26.04.2023).

12. Libro Blanco de Defensa Nacional de Brasil, 2012. 282 p.

13. NETmundial Multistakeholder Statement // NETmundial. URL: https://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (дата обращения: 26.04.2023).

14. NETmundial – Dilma Rouseff's Opening Speech // NETmundial. URL: https://netmundial.br/wp-content/uploads/2014/04/NETMundial-23April2014-Dilma-Rousseff-Opening-Speech-en.pdf (дата обращения: 26.04.2023).

Клестова Валерия Александровна
магистрант
Санкт-Петербургский государственный университет,
Факультет международных отношений
E-mail: st084548@student.spbu.ru

ЦИФРОВЫЕ ПЛАТФОРМЫ В МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Аннотация. *Актуальность обуславливается всё большей цифровизацией общества. Современные технологии всё теснее вплетаются во все сферы жизни под идеей решить любую проблему. Поэтому неудивительно, что государства также стремятся использовать их. Новизна данной работы заключается в том, что в основном изучается экономическая роль цифровых платформ, однако почти нет работ, посвящённых роли этих платформ в международных отношениях. В докладе рассмотрены цифровые платформы как явление. Рассмотрены некоторые виды платформ, в том числе государственные цифровые платформы. Также показаны примеры того, как государства могут использовать цифровые платформы для продвижения своей политики.*

Ключевые слова: *международные отношения, цифровые платформы, данные, цифровая экономика, электронное правительство, цифровой разрыв, Закон о цифровых услугах, Закон о цифровых рынках*.

Цифровые платформы как феномен. Канадский экономист Ник Срничек описывает современную экономику как информационную, где главным сырьём являются данные [6, С. 36-37]. Развитие и распространение компьютеров делают такую экономику ещё и цифровой, которая, в свою очередь, становится неотъемлемым элементом мировой экономики. Кроме того, проникновение цифровых технологий обосновывается мыслями об идеальном обществе: города должны быть умными, рабочие – приспосабливающимися (странновато звучит, рекомендую подумать над заменой слова), а правительства – интеллектуальными [6, С. 11].

Как уже отмечалось, главным сырьём являются данные, т.е. информация об окружающем мире. Эти данные необходимо извлечь и обработать, для чего создаётся мощная инфраструктура. И таким образом, тот, кто больше получает данных, получает и большие возможности [6, С. 42-43]. Это привело к появлению платформ, цифровых инфраструктур, которые выполняют роль посредников и благодаря которым группы пользователей могут взаимодействовать [6, С. 41]. В качестве примера можно привести такие компании как Alphabet (ранее Google – *прим*.), Apple, Microsoft, Meta* и др. Цель платформ – привлечь как можно больше пользователей. В свою очередь, большее число пользователей подталкивает платформы к образованию монополии, поскольку расширение количества пользователей приводит к расширению деятельности и ещё большему накоплению данных в связи с их значимостью. Американский философ Шошана Зубофф считает, что корпорации начали соревнование или так называемую «гонку вооружений» по развитию технологий, в частности искусственный интеллект, которые бы могли извлекать больше данных. Для этого они привлекают множество специалистов, а также поглощают другие, более мелкие компании [1, С. 250].

Ник Срничек выделяет 5 типов цифровых платформ. **Рекламные платформы**, собирающие данные о пользователях, анализируют их и продают рекламодателям (Alphabet и Meta) [6, С. 47]. **Облачные платформы**, создающие и сдающие в аренду инфраструктуру тем, чья деятельность связана с цифровой сферой (Adobe и Microsoft) [6, С. 57]. **Промышленные платформы**, создающие оборудования и программные обеспечения, необходимые для перехода из традиционного производства в Интернет-пространство для крупных промышленных предприятий (General Electric и Siemens) [6, С. 47]. **Продуктовые платформы**, трансформирующие с помощью платформ товары в услуги и сдающие их в аренду «по требованию» (цифровые библиотеки и Spotify) [6, С. 65]. **Бережливые платформы**, минимизирующие объём активов, находящихся в собственности для сокращения издержек (Uber и Booking.com) [6, С. 47]. Такой вид модели ещё

называется гипераутсорсингом, т.е. на платформах работают подрядчики, а не наёмные работники [6, С. 69].

В этот список стоит ещё добавить **государственные цифровые платформы**. Главной их особенностью является то, что за жизнеспособность и функционирование ответственен государственный орган [7, С. 11]. Также государственные цифровые платформы не стремятся захватить как можно большую долю рынка. Вместо этого эффективность платформы оценивается с точки зрения общественной важности [7, С. 9]. При этом в отличие от коммерческих платформ, которые могут себе позволить скрывать механизм работы своих алгоритмов, государственные цифровые должны быть прозрачными и открытыми, и в то же время достаточно надёжными, чтобы вызывать доверие у общества и повышать тем самым свою ценность [7, С. 12]. При этом такая классификация цифровых платформ не является единственной и общепринятой. Однако для данного исследования была выбрана имена такая классификация, поскольку она поможет выявить самые влиятельные цифровые платформы.

Важно отметить, что крупнейшие технологические компании, например, Apple, Meta*, Alphabet, Amazon и Microsoft стремятся решить любую проблему общества с помощью технологий. Такое стремление основано на убеждении, что любую проблему можно представить как набор задач, для решения которых нужно подобрать верные алгоритмы [13, P. 9]. Именно это обуславливает проникновение цифровых технологий во все сферы жизни, начиная от рутины и заканчивая политикой.

Цифровые технологии в международных отношениях. Если говорить о международных отношениях, то здесь цифровые платформы могут помогать государствам распространять своё влияние и на другие государства. Например, Первая поправка к Конституции США гарантирует, что государство не будет посягать на свободу слова. Это даёт возможность гражданам США использовать так называемый «язык ненависти» (hate speech). Что же касается ЕС, то Союз борется с «языком ненависти» и

преступлениями на почве ненависти. При этом ЕС удаётся распространить свою борьбу и на США. Это проявляется в том, что в 2016 году ЕС заключил соглашение с такими компаниями как Meta, YouTube, Twitter и Microsoft. Суть заключается в том, что эти компании должны применять европейские нормы на своих платформах, в том числе и нормы по борьбе с дискриминационным контентом [10]. Ещё одним примером является Закон о цифровых услугах (the Digital Services Act, DSA). Закон обязывает платформы регулировать свой контент, а также проводить ежегодные независимые аудиты о своей деятельности по борьбе с вредоносным контентом [12]. Кроме того, Европейской комиссией был принят так называемый Закон о цифровых рынках (the Digital Markets Act, DMA). Этот закон ограничивает монополию техногигантов и может принуждать цифровые платформы разрешать устанавливать сторонние программы, раскрывать свои конфиденциальной информацией для конкурентов этих самых платформ. При этом закон затрагивает все компании, которые ведут бизнес в ЕС, американские под исключение не попадают [15]. Принятие Закона о цифровых рынках вызвало обеспокоенность не только у американских частных компаний, но и у Администрации Президента США. Президент США Джо Байден был вынужден написать обращение в Еврокомиссию с просьбой пересмотреть данный закон. В Администрации считают этот закон антиамериканским и нацеленным именно на американские компании [14]. Это приводит к тому, что европейские нормы распространяются за пределами ЕС, поскольку компаниям тяжело разграничивать европейских регион от остального мира. И таким образом, ЕС через цифровые платформы распространяет своё влияние, обходя законы США.

Не менее важную роль играют цифровые платформы в отношении развитых и развивающихся стран. Дело в том, что вопрос о неоколониализме

поднимает политолог Иван Владимирович Данилин[2]. Так, большинство достижений в сфере высокотехнологичной отрасли всё ещё приходится на развитые страны. Развивающейся страны, несмотря на свои успехи в данной отрасли, всё ещё остаются получателями технологий. Такое положение может привести к асимметрии в отношениях между развитыми и развивающимися странами. Тем самым, есть риск, что последние окажутся в более тонких формах зависимости [11]. Того же мнения придерживается исследователь Центра политических исследований ОАЭ (Emirates Policy Center) Самир Рамзи[3]. В ходе экспертной дискуссии в Фонде поддержки публичной дипломатии имени А.М. Горчакова он назвал такое явление «цифровым разрывом» («digital-gap»). Развитые страны концентрируют у себя ресурсы и технологии, а также препятствуют конкуренции, не допуская до рынка платформы, созданные в развивающихся странах [3].

Тот же И.В. Данилин считает, что в долгосрочной перспективе цифровые платформы и искусственный интеллект смогут играть свою роль в международных дискуссиях [11]. Это может привести к трансформации самих международных отношений в той части, что к этим дискуссиям будут привлекаться общественность и эксперты, т.е. принятие решений будет находиться не только у государств. Этот прогноз уже сбывается. В качестве примера можно привести создание Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021-2025. Благодаря открытости в заседаниях с целью обмена мнениями могут принимать участие другие заинтересованные стороны, такие как бизнес, НПО и научно-экспертное сообщество [4]. Также есть вероятность, что традиционные бумажные договоры будут заменены смарт-контрактами и кодексами поведения [11].

---

[2] Иван Владимирович Данилин - Заведующий сектором инновационной политики, Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук.

[3] Самир Рамзи - Исследователь Центра политических исследований ОАЭ, независимого аналитического центра ОАЭ.

Интересна также роль цифровых платформ в управлении государством. Так, существует Академия электронного управления или eGA. Это инициатива правительства Эстонии, Института открытого общества и Программы Развития ООН. Целью eGA является планирование и разработка электронного правительства, а также помогает в переходе к цифровым технологиям в государственном управлении. Организация создала цифровое правительство Эстонии, но также готова делиться своим опытом и с другими государствами [2]. Также разрабатываются межгосударственные проекты. В период 2014-2015 годах проводился проект по сотрудничеству налоговых департаментов стран Балтийского моря или BSR Taxi. Проект проводился между Латвией, Эстонией и Швецией. Общая база данных позволила не только скоординировать действия стран-участниц в сфере уклонения от уплаты налогов, но и также составить анализ законодательств стран и сильных и слабых сторон в существующих системах стран-участниц [5]. Ещё одним примером можно назвать проект по совместной экспериментальной разработке политики или Европа, принимающая решения совместно (Co-Deciding Europe). В проекте принимают участие Эстония, Исландия, Латвия, Португалия, Греция, Бельгия, Болгария, Венгрия и Словения. В качестве экспериментального направления выбрано качество воздуха. Цель проекта – развитие цифровой демократии путём большего вовлечения граждан в процесс принятия решения [8]. Для этого предлагается устраивать общественные слушания и мозговые штурмы, в ходе которых собираются большие данные, например, описание проблем, с которыми сталкиваются граждане стран-участниц, или предложения решения этих самых проблем [9]. Из этого следует, что рассмотренные проекты показывают, как государственные цифровые платформы могут расшириться за рамки одного государства и координировать совместные действия государств в определённых вопросах.

Заключение. Таким образом, данная работа частично освещает потенциал, который имеют современные технологии, и даёт основное

понимание места цифровых технологий в международных отношениях и то, как они могут их трансформировать. Кроме того, некоторые из приведённых примеров представляют собой интересный опыт, который может быть полезен для России, особенно в части координации между государствами в различных сферах. Это позволит улучшить взаимодействия между регионами государств по значимым для них направлениях.

*Организация Meta признана экстремистской по решению суда, деятельность организации запрещена на территории Российской Федерации.

Список источников и литературы:

1. Зубофф, Ш. Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти / Шошана Зубофф; пер. с англ. А.Ф.Васильева; под ред. Я.Охонько и А.Смирнова. — Москва: Издательство Института Гайдара, 2022. — 784 с.;

2. Об академии / E-Governance Academy. [Электронный ресурс] // URL: https://ega.ee/ru/about-us/ (дата обращения: 24.04.2023);

3. О цифровых платформах в международных отношениях сегодня: в Фонде Горчакова прошла экспертная дискуссия [экспертная дискуссия в Фонде Горчакова] / Фонд Горчакова. 16.05.2022. [Электронный ресурс] // URL: https://gorchakovfund.ru/portal/news/view/o_tsifrovykh_platformakh_v_mezhdunarodnykh_otnosheniiakh_segodnia_v_fonde_gorchakova_proshla_ekspertnaia_diskussiia_59816 (дата обращения: 24.04.2023);

4. Резолюция, принятая Генеральной Ассамблеей 31 декабря 2020 года. A/RES/75/240. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. [Электронный ресурс] // URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement (дата обращения: 28.06.2023);

5. Сотрудничество налоговых департаментов в регионе Балтийского моря / E-Governance Academy. [Электронный ресурс] // URL:

https://ega.ee/ru/project/sotrudnichestvo-nalogovyh-departamentov-v-regione-baltijskogo-morya/ (дата обращения: 24.04.2023);

6. Срничек, Н. Капитализм платформ [Текст] / пер. с англ. и науч. ред. М. Добряковой; Нац. исслед. ун-т «Высшая школа экономики». — М.: Изд. дом Высшей школы экономики, 2019. — 128с.;

7. Стырин, Е.М., Дмитриева, Н.Е. Государственные цифровые платформы: ключевые особенности и основные сценарии развития [Текст] : докл. к XXII Апр. междунар. научн. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / Е. М. Стырин, Н. Е. Дмитриева; Нац. исслед. ун-т «Высшая школа экономики». — М.: Изд. дом Высшей школы экономики, 2021. — 32 с.;

8. Экспериментальная совместная разработка политики / E-Governance Academy. [Электронный ресурс] // URL: https://ega.ee/ru/project/eksperimentalnaya-sovmestnaya-razrabotka-politiki/ (дата обращения: 24.04.2023);

9. CODE EUROPE / Официальная страница проекта Co-Deciding Europe. [Электронный ресурс] // URL: https://codecidingeurope.eu (дата обращения: 24.04.2023);

10. Combating hate speech and hate crime Measures to prevent and combat different forms of hatred and to protect victims / European Commission. [Электронный ресурс] // URL: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/combating-hate-speech-and-hate-crime_en (дата обращения: 24.04.2023);

11. Danilin, I. Emerging Technologies And Their Impact On International Relations And Global Security. Hoover Institution. 03.10.2018. [Электронный ресурс] // URL: https://www.hoover.org/research/emerging-technologies-and-thei.r-impact-international-relations-and-global-security (дата обращения: 24.04.2023);

12. Milmo, D. Digital Services Act: inside the EU’s ambitious bid to clean up social media / The Guardian. 17.12.2022. [Электронный ресурс] // URL: https://www.theguardian.com/media/2022/dec/17/digital-services-act-inside-the-eus-ambitious-bid-to-clean-up-social-media (дата обращения: 24.04.2023);

13. Morozov, E. To save everything, click here. The folly of technological solutionism. — New York, PublicAffairs, 2013. — 415 p.;

14. Stolton, S. US pushes to change EU’s digital gatekeeper rules / Politico. 31.01.2022. [Электронный ресурс] // URL: https://www.politico.eu/article/us-government-in-bid-to-change-eu-digital-markets-act/ (дата обращения: 24.04.2023);

15. Wall, C., Lostri, E. The European Union’s Digital Markets Act: A Primer / CSIS. 08.02.2022. [Электронный ресурс] // URL: https://www.csis.org/analysis/european-unions-digital-markets-act-primer (дата обращения: 24.04.2023).

Елизавета Викторовна Мищишина
магистр ФМП МГУ им. М.В.Ломоносова
E-mail: lizavetta.mish@gmail.com

ЦИФРОВИЗАЦИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ: УГРОЗЫ И РИСКИ ДЛЯ ЯПОНИИ

Аннотация. *В рамках работы были проанализированы риски цифровизации международных отношений на примере Японии. Автором было проведено два исследования, направленных на выявление подходов Японии к использованию социальных сетей, а также проведен анализ причин, тормозящих процесс цифровизации. На основе анализа автором были сделаны выводы о недостатках японского подхода к внедрению цифровых технологий.*

Ключевые слова: *Япония, цифровые технологии, информационная безопасность, цифровая дипломатия, внешняя политика.*

Цифровые технологии стали неотъемлемой частью внешней политики Японии и других стран. Япония, как лидер в сфере технического прогресса, достигает внешнеполитических задач и устанавливает дипломатические связи, используя современные цифровые решения. Цифровизация помогает стране укреплять национальную безопасность, получать лидерство на мировой арене и становиться успешной экономической державой. Изучение цифровых технологий во внешней политике Японии позволяет более глубоко понять ее политическую стратегию и дипломатический подход, что, в свою очередь, дает возможность построить модель эффективного взаимодействия.

Кибератаки, информационные войны и разведка становятся основными проблемами в международных отношениях. В связи с этим, важным становится обеспечение международной информационной безопасности, которая выходит на первый план. Одной из ключевых задач в этой области становится контроль за информационным пространством, регулируемым

многосторонними отношениями, так как ответственность за цифровой мир лежит на каждом участнике международного сообщества [1].

Япония стремительно развивается в цифровом мире, что обуславливает изменение правового регулирования гражданских прав и активно развивает правовое регулирование технологий, чтобы обеспечить безопасность и защиту в цифровом пространстве. В отличие от представлений западных стран, Япония не рассматривает Интернет как свободное пространство для самовыражения и свободного обмена информацией. Для продвижения своей концепции Япония использует культурную дипломатию и экономические возможности, такие как информационные проекты, связанные с концепцией «Крутая Япония» («Cool Japan», CJ).

Однако, несмотря на успехи технической части и активное внедрение цифровых технологий, в японском обществе существуют несколько национальных особенностей, препятствий, которые тормозят процесс.

Во-первых, сам японский язык. Его набор символов кандзи (в дополнение к алфавиту для японской письменности требуется несколько сотен графически различимых каллиграфических знаков), что было и остается значительным препятствием для широкого внедрения информационных технологий.

Во-вторых, японская бизнес-культура может стать препятствием для инноваций. Япония славится своими очень формализованными иерархическими структурами, где решения принимаются сверху вниз, и критика или несогласие с руководством не приветствуются.

Третьим ключевым элементом японской бизнес-культуры являются нормы и ценности, которые акцентируют внимание на организационных и человеческих аспектах обработки информации. К примеру, новички в компании обязательно полагаются на помощь и советы своих коллег в поиске необходимой информации, а также для понимания правил и процедур [2].

Пандемия COVID-19 подняла одну из главных проблем – медленный темп цифровизации административных услуг, включая сложные процедуры и задержки выплат пособий. Из-за только частично оптимизированных ИТ-систем национального правительства цифровизация проходит медленно., Многие административные заявки до сих пор нельзя подать онлайн, что продолжает тормозить процесс цифровизации. Среди главных задач, изложенных в плане, обеспечение всех жителей Японии ID-картами. Еще одной важной целью является создание информационных систем, совместимых с новыми технологиями, что будет достигнуто путем использования облачных сервисов [3].

Тем не менее, в настоящее время Япония активно занимается разработкой законодательства, связанного с телекоммуникациями и информационными технологиями. В Японии существует налаженная правовая база, охватывающая широкий спектр индустрий, связанных с информационно- телекоммуникационной отраслью.

Однако, определенные проблемы все же остаются, такие как неоднородность регулирования отраслей, что препятствует развитию малых предприятий, которые не могут выдержать возросшие нормативно-правовые требования. объективным и учитывать интересы всех заинтересованных сторон. В Японии наблюдается тенденция к созданию жесткого правового режима для защиты информации в Интернете. В частности, Япония ориентирована на создание законов, которые бы ограничивали возможность хакеров получить незаконный доступ к информации в Интернете, гарантируя безопасность и персональную защиту пользователей [4].

Одной из главных целей японской цифровой дипломатии является распространение информации о внешней политике Японии и популяризация японской культуры среди зарубежной аудитории. Для этого Япония создает анимационные проекты, которые могут быть интересными для людей по всему миру, показывая традиционные японские ценности и эстетику. Также

производится активное продвижение туристических и культурных проектов в медиапространстве. Брендинг страны имеет ключевое значение в развитии цифровой дипломатии.

В рамках работы автором было проведено два исследования, направленных на выявление подходов Японии к использованию социальных сетей. В рамках первой работы нами был проведен семантический анализ публичных комментариев на странице JNTO в Facebook с июля 2022 г. по декабрь 2022 г. [5]. Аккаунт набрал 790 000 подписчиков в декабре 2022 года. Всего было отобрано 537 комментариев, содержащих текстовую информацию. На основе этого был проведен семантический анализ, который выявил следующее. Наиболее часто используемым ключевым словом в сети JNTO стало слово «Япония» (96), за которым следовали слова «прекрасный» (74), «визит» (41), «приятный» (25), «удивительный» (23), «любовь» (23), «японский» (18), «чудесный» (16), «вишневый» (13), «место» (12), «вау» (12), «страна» (12), «путешествие» (12), «опыт» (11), «международный» (10), «абсолютно» (10), «надежда» (10), «цвести» (10), «годы» (10) и т.д.

В Таблице 1 приведен список ключевых слов в комментариях. Данные комментарии подчеркивают, что для аудитории Япония была символом красоты и уникальности, при этом положительное восприятие страны связывалось с обширным перечнем туристических достопримечательностей, которые были посещены посетителями. Общие темы, которые могут быть выделены из ключевых слов, включают в себя увлечение туризмом, впечатление от привлекательной природы Японии, путешествия и обмен личным опытом. Метод семантического анализа показал, что комментарии преимущественно выражают положительные эмоции и первые впечатления о Японии, которая поражает своей удивительной природой, туристическими достопримечательностями и общим уровнем удовлетворенности посещения страны.

Таблица 1. Семантический анализ комментариев с официального Facebook Japan National Tourism Organization (JNTO) за июль-декабрь 2022 г.

№	Word	Слово	Кол-во	Релевантность	% в ядре	% в тексте
1	japan	Япония	96	8.48	4.5%	2.3%
2	beautiful	прекрасный	74	6.54	3.5%	1.7%
3	visit	визит	41	3.62	1.9%	0.9%
4	nice	приятный	25	2.2	1.1%	0.6%
5	amazing	удивительный	23	2.03	1%	0.5%
6	love	любовь	23	2.03	1%	0.5%
7	japanese	японский	18	1.59	0.8%	0.4%
8	wonderful	чудесный	16	1.41	0.7%	0.3%
9	cherry	вишневый	13	1.14	0.6%	0.3%
10	place	место	12	1.06	0.5%	0.2%
11	wow	вау	12	1.06	0.5%	0.2%
12	country	страна	12	1.06	0.5%	0.2%
13	travel	путешествие	12	1.06	0.5%	0.2%
14	experience	опыт	11	0.97	0.5%	0.2%
15	international	международный	10	0.88	0.4%	0.2%
16	absolutely	абсолютно	10	0.88	0.4%	0.2%
17	hope	надежда	10	0.88	0.4%	0.2%
18	blossoms	цвести	10	0.88	0.4%	0.2%
20	years	годы	10	0.88	0.4%	0.2%
21	great	великолепный	9	0.79	0.4%	0.2%
22	kyoto	Киото	9	0.79	0.4%	0.2%
23	awesome	потрясающий	9	0.79	0.4%	0.2%
24	tokyo	Токио	8	0.7	0.3%	0.1%
25	more	больше	8	0.7	0.3%	0.1%
26	people	люди	8	0.7	0.3%	0.1%
27	autumn	осень	8	0.7	0.3%	0.1%
28	interesting	интересный	8	0.7	0.3%	0.1%
31	tour	тур	7	0.61	0.3%	0.1%
32	trip	поездка	7	0.61	0.3%	0.1%
33	details	детали	7	0.61	0.3%	0.1%
34	yummy	вкусно	7	0.61	0.3%	0.1%

36	water	вода	6	0.53	0.2%	0.1%
37	looks	выглядеть	6	0.53	0.2%	0.1%
41	visited	посетил	6	0.53	0.2%	0.1%
42	gorgeous	невероятный	6	0.53	0.2%	0.1%
43	park	парк	6	0.53	0.2%	0.1%
44	loved	любимый	5	0.44	0.2%	0.1%
45	super	супер	5	0.44	0.2%	0.1%
46	wish	желание	5	0.44	0.2%	0.1%
47	april	апрель	5	0.44	0.2%	0.1%
49	dream	мечта	5	0.44	0.2%	0.1%
50	tourists	туристы	5	0.44	0.2%	0.1%

Источник: Japan National Tourism Organization (JNTO). URL: https://www.facebook.com/visitjapaninternational/ (дата обращения: 25.03.2023)

В рамках второго исследования был проведен анализ коэффициентов вовлеченности аккаунта (Engagement Rate) Фумио Кисиды в Twitter за период с 23.12.2022 по 23.01.2023. Всего было проанализировано 38 постов, опубликованных на странице премьер-министра за этот период. На аккаунт подписаны 698 900 человек. В Таблице 2 представлен анализ постов аккаунта Фумио Кисиды в Twitter. Определено количество комментариев, количество репостов, количество лайков, суммарное количество реакций, количество просмотров для каждого поста. А также подведена общая сумма реакций для всех постов за рассматриваемый период.

Таблица 2. Анализ постов с аккаунта Фумио Кисиды в Twitter за период с 23.12.2022 по 23.01.2023

	Ссылка на пост	**Кол-во комментариев (в ед.)**	**Кол-во репостов (в ед.)**	**Кол-во лайков (в ед.)**	**Суммарное кол-во реакций (в ед.)**	**Кол-во просмотров (в ед.)**
1.	https://twitter.com/kishida230/status/1605560501513072640?s=20	4311	1801	6038	12150	1800000
2.	https://twitter.com/JMA_bousai/status/1606498199283589121?s=20	351	505	952	1808	558900
3.	https://twitter.com/kishida230/status/1607374637012496386?s=20	4556	989	2112	7657	1200000
4.	https://twitter.com/kishida230/status/1608692336170774528?s=20	201	515	3878	4594	459200
5.	https://twitter.com/kishida230/status/1608692334186885123?s=20	540	4631	65300	70471	2700000
6.	https://twitter.com/kishida230/status/1608798936365666307?s=20	3021	1519	4145	8685	2500000
7.	https://twitter.com/kishida230/status/1609217069035433986?s=20	424	391	1488	2303	431700
8.	https://twitter.com/kishida230/status/1609217067491950592?s=20	4164	3310	20400	27874	3200000
9.	https://twitter.com/kishida230/status/1609488168600096769?s=20	5134	3157	22800	31091	4000000
10.	https://twitter.com/kishida230/status/1610502241110339584?s=20	2269	2241	17800	22310	3300000

11.	https://twitter.com/kishida230/status/1610634295961612288?s=20	559	236	915	1710	271700
12.	https://twitter.com/kishida230/status/1610634291872165888?s=20	2284	1182	5545	9011	1200000
13.	https://twitter.com/kishida230/status/1611000319093374976?s=20	2372	1024	3376	6772	1500000
14.	https://twitter.com/kishida230/status/1611347110858981377?s=20	228	184	721	1133	208700
15.	https://twitter.com/kishida230/status/1611347104479469569?s=20	2297	1076	3390	6763	1800000
16.	https://twitter.com/kishida230/status/1612106268214431745?s=20	1704	1058	4326	7088	877700
17.	https://twitter.com/kishida230/status/1612355292284743681?s=20	2711	1997	7841	12549	1700000
18.	https://twitter.com/kishida230/status/1612355984823025665?s=20	2742	2268	10000	15010	4900000
19.	https://twitter.com/kishida230/status/1612489737956397063?s=20	560	449	2203	3212	377300
20.	https://twitter.com/kishida230/status/1612608131410067457?s=20	972	915	3755	5642	715600
21.	https://twitter.com/kishida230/status/1612740172394946563?s=20	248	237	1089	1574	219700
22.	https://twitter.com/kishida230/status/1612740168511008769?s=20	501	493	2505	3499	359800

23.	https://twitter.com/kishida230/status/1612894618189983745?s=20	189	203	1048	1440	196600
24.	https://twitter.com/kishida230/status/1612894616487067648?s=20	383	364	1726	2473	596700
25.	https://twitter.com/kishida230/status/1612966340016640000?s=20	1432	908	3697	6037	1000000
26.	https://twitter.com/kishida230/status/1613330697326067712?s=20	238	722	2627	3587	562700
27.	https://twitter.com/kishida230/status/1613330686605422592?s=20	1122	1194	4978	7294	1300000
28.	https://twitter.com/kishida230/status/1613402230346108931?s=20	268	251	1176	1695	199400
29.	https://twitter.com/kishida230/status/1613402222347571207?s=20	541	386	1802	2729	643700
30.	https://twitter.com/kishida230/status/1613739813651517440?s=20	164	252	1003	1419	176700
31.	https://twitter.com/kishida230/status/1613739801605451777?s=20	846	874	3643	5363	1000000
32.	https://twitter.com/kishida230/status/1613754341504208897?s=20	356	208	791	1355	202400
33.	https://twitter.com/kishida230/status/1613754339147026433?s=20	536	313	1407	2256	552300
34.	https://twitter.com/kishida230/status/1614149258688729090?s=20	2720	1701	6458	10879	1800000

35.	https://twitter.com/kishida230/status/1614422899401822208?s=20	1448	377	1363	3188	401900
36.	https://twitter.com/kishida230/status/1614422897556336640?s=20	1855	552	2213	4620	1000000
37.	https://twitter.com/kishida230/status/1616399256017043458?s=20	3172	1122	3064	7358	1200000
38.	https://twitter.com/kishida230/status/1617536948050202624?s=20	10400	4627	7299	22326	3000000
Общая сумма		67819	44232	234874	346925	48112700

Источник: Twitter Фумио Кисиды https://twitter.com/kishida230 (дата обращения: 05.04.2023).

В Таблице 3 подсчитаны коэффициенты вовлеченности аккаунта Фумио Кисиды. Если рассматривать средние показатели, то коэффициенты вовлеченности получается следующим: для комментариев на один пост 0.26%, для репостов на один пост 0.17%, для лайков на один пост 0.88%, для реакций на один пост 1.31%, для просмотров на один пост 181.16%.

Таблица 3. Коэффициенты вовлеченности аккаунта Фумио Кисиды в Twitter за период с 23.12.2022 по 23.01.2023

Кол-во подписчиков (в ед.)	**Критерий**	**Коэффициенты вовлеченности в %**
698 900	Кол-во комментариев – 67 819	9.7%
698 900	Кол-во репостов – 44 232	6.33%
698 900	Кол-во лайков – 234 874	33.61%
698 900	Суммарное кол-во реакций – 346 925	49.64%

698 900	Кол-во просмотров – 48 112 700	6884.06%
698 900	Среднее кол-во комментариев на один пост – 1 784	0.26%
698 900	Среднее кол-во репостов на один пост – 1 164	0.17%
698 900	Среднее кол-во лайков на один пост – 6 180	0.88%
698 900	Среднее кол-во реакций на один пост – 9 129	1.31%
698 900	Среднее кол-во просмотров на один пост – 1 266 123	181.16%

В Таблице 4 представлены коэффициенты вовлеченности для самого популярного и наименее популярного поста в аккаунте. Самая популярная публикация – это новогодняя фотография премьер-министра с императрицей и поздравление с Новым годом [6]. Конверсия составляет: для комментариев на один пост 0.73%, для репостов на один пост 0.45%, для лайков на один пост 3.26%, для реакций на один пост 4.45%, для просмотров на один пост 572.33%. Самая непопулярная публикация – это запись о телефонном разговоре с Президентом Украины Владимиром Зеленским. Запись говорит следующее: «Я заявил, что Япония будет играть активную роль в качестве председательства в «Большой семерке» и приложит максимум усилий для оказания помощи, в том числе зимней поддержки, для защиты жизни людей Украины» [7]. Конверсия составляет: для комментариев на один пост 0.03%, для репостов на один пост 0.03%, для лайков на один пост 0.1%, для реакций на один пост 0.16%, для просмотров на один пост 29.86%.

Таблица 4. Коэффициенты вовлеченности самого популярного и наименее популярного поста в аккаунте Фумио Кисиды в Twitter за период с 23.12.2022 по 23.01.2023

Самый популярный пост		
Кол-во подписчиков	**Критерий**	**Коэффициенты вовлеченности в %**
698 900	Кол-во комментариев – 5134	0.73%
698 900	Кол-во репостов – 3157	0.45%
698 900	Кол-во лайков – 22800	3.26%
698 900	Суммарное кол-во реакций – 31 091	4.45%
698 900	Кол-во просмотров – 4 000 000	572.33%
Наименее популярный пост		
Кол-во подписчиков	**Критерий**	**Коэффициенты вовлеченности в %**
698 900	Кол-во комментариев – 228	0.03%
698 900	Кол-во репостов – 184	0.03%
698 900	Кол-во лайков – 721	0.1%
698 900	Суммарное кол-во реакций – 1 133	0.16%
698 900	Кол-во просмотров – 208 700	29.86%

Для понимания конверсии возьмем ранжирование показателей SMM-специалистов, который определяют следующие показатели: менее 1% — плохо; от 1% до 3,5% — среднее значение; от 3,5% до 6% — хороший уровень; свыше 6% — отличный коэффициент (данные актуальны для реакций). На основании этого мы можем сделать следующие выводы по исследованию. Аккаунт японского премьер-министра собирает большое количество просмотров и лайков, однако, для такого количества подписчиков недостаточно комментарийной активности. Веб-страница ведется

преимущественно на японском языке, что затрудняет коммуникацию с международной аудиторией. Больше реакций набирают публикации, связанные с внутренней повесткой, что демонстрирует ориентированность японского общества «внутрь страны».

Заключение. Результаты, полученные в ходе проведенного исследования, подтверждают следующее. Во-первых, цифровизация в Японии происходит медленно из-за национальных особенностей, которые тормозят этот процесс. Из-за волокиты с документами процесс внесения изменений в законодательство тормозится. Во-вторых, одной из основных задач японской цифровой дипломатии является распространение информации о внешней политике страны и знакомство с культурой Японии в целях улучшения взаимопонимания в мире. Несмотря на активное использование социальных сетей, у японской цифровой дипломатии наблюдается отсутствие непосредственного взаимодействия с интернет-пользователями, и социальные сети используются преимущественно как инструмент для распространения информации, но не для установления значимых связей с аудиторией. Следует также упомянуть недостаток англоязычных социальных сетей у японских агентств.

Список источников и литературы:

1. Danilin I.V. Emerging Technologies And Their Impact On International Relations And Global Security // Hoover Institution. URL: https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security (дата обращения: 19.03.2023).

2. Digital Transformation in Japan/ Assessing business opportunities for EU SMEs. URL: https://www.eu-japan.eu/sites/default/files/publications/docs/Digital-Transformation-Japan-Assessing-opportunities-forEU-SMEs.pdf (Дата обращения: 14.12.2022).

3. Japan: Diet Passes Three New Laws to Promote a "Digital Society" // Library of Congress. URL: https://www.loc.gov/item/global-legal-monitor/2021-

07-23/japan-diet-passes-three-new-laws-to-promote-a-digital-society/ (дата обращения: 12.04.2023).

4. Савинцева М.И. Информационное общество и основы правового регулирования и развития информационно-телекоммуникационной индустрии в Японии // Ежегодник Япония. 2008. №37. URL: https://cyberleninka.ru/article/n/informatsionnoe-obschestvo-i-osnovy-pravovogo-regulirovaniya-i-razvitiya-informatsionno-telekommunikatsionnoy-industrii-v-yaponii (дата обращения: 29.03.2023).

5. Аккаунт в Facebook Japan National Tourism Organization (JNTO). URL: https://www.facebook.com/visitjapaninternational/ (дата обращения: 25.03.2023).

6. Пост 1 из аккаунта Фумио Кисиды. URL: https://twitter.com/kishida230/status/1609488168600096769?s=20 (дата обращения: 29.03.2023). 105

7. Пост 2 из аккаунта Фумио Кисиды. URL https://twitter.com/kishida230/status/1611347110858981377?s=20 (дата обращения: 29.03.2023).

Пичугин Николай Васильевич
стажёр-исследователь
Институт статистических исследований и экономики знаний Высшей школы экономики
E-mail: nikolaivpichugin@gmail.com

ГЛОБАЛЬНЫЕ ВЫЗОВЫ И УГРОЗЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КНР

Аннотация. *Внимание уделяется актуальным для Китайской Народной Республики вызовам и угрозам в сфере информационной безопасности. Акцент делается на проблеме правового регулирования искусственного интеллекта, а также на вопросе злонамеренного использования информационно-коммуникативных технологий. Исследуются подход и конкретные шаги китайского руководства по урегулированию выделенных вызовов и угроз.*

Ключевые слова: *информационная безопасность, вызовы и угрозы, нормативно-правовое регулирование, ИКТ, ИИ, DDOS-атака (Denial-of-service attack), дипфейк (深度合成, deep synthesis), внезапная кибератак (突发性网络攻击, sudden cyber attack), КНР.*

По мере развития информационно-коммуникативных технологий (ИКТ), искусственного интеллекта (ИИ), больших данных и других цифровых технологий, повсеместно участились случаи появления новых угроз в информационном пространстве. В Китайской Народной Республики (КНР), с одной стороны, распространены вызовы, характерные для стран с высоким уровнем цифрового развития, такие как недостаточный уровень правового регулирования информационного пространства, которое не поспевает за скоростью развития последнего. С другой стороны, ввиду особенностей и специфики общей китайской модели цифрового управления и кибербезопасности, для неё свойствен ряд определённых отдельных угроз.

Актуальность темы исследования обусловлена необходимостью усовершенствования и создания в Российской Федерации собственной цифровой системы государственного управления информационной безопасности, обеспечения её суверенитета и безопасности ключевых объектов цифровой инфраструктуры на фоне разворачивающейся гибридной технологической войны против российского государства и его систем жизнеобеспечения. В Китае отказались от всестороннего использования западных цифровых технологий в обеспечении национальной системы информационной безопасности, что позволило не только разработать собственные и создать независимую цифровую институциональную модель, но и эффективно защитить национальный суверенитет в исследуемой сфере. Прогрессивный управленческий опыт китайского государства является ярким примером национально-ориентированной государственной политики в области цифрового строительства, и он чрезвычайно актуален для России, которая столкнулась с необходимостью создания, по примеру КНР, независимой от Запада системы информационной безопасности.

Научная новизна исследования заключается в том, что в отечественной научной и практической литературе в основном подробно исследуются технологические или общие политические аспекты китайской системы регулирования в сфере информационной безопасности, однако за рамками внимания остаются фундаментальные особенности институционального строительства и правой системы, на которых также основывается технический прогресс Китая.

Цель работы заключается в выделении глобальных вызовов и угроза в сфере информационной безопасности и установлении подхода руководства КНР к их преодолению на основе специфики собственной системы правового регулирования и цифрового развития.

Глобальные вызовы в лице так называемых DDOS-атак (Denial-of-service) и их подвида «внезапных кибератак» (**突**发性网络攻击, sudden cyber attack) [6,

С. 148], а также вопросов правового регулирования ИИ, включающих угрозу в виде «дипфейков» (**深度合成**, deep synthesis), являются одними из наиболее обсуждаемых и серьёзных тем, как во внутренней китайской политике, так и на международном уровне [7, С. 74].

Положения «Всестороннего плана построения цифрового Китая» (**数字中国建**设整体布局规划) [5], а также части «XIV пятилетнего плана», посвященной цифровизации («**十四五**» **国家信息化**规划) [4], свидетельствуют, что в Китае разрабатываются стратегии для эффективного противодействия всем видам DDOS-атак. Отдельного внимания заслуживает создаваемое в настоящее время в рамках проектов по усовершенствованию китайской цифровой инфраструктуры Национальное управление данных (**国家数据局**) при Национальной комиссии по развитию и реформам КНР (**中**华人民共和国国家发展和改革委员会的创新和高技术发展司). В будущем его работа может позволить достаточно значительно сократить время, необходимое соответствующим китайским структурам на реагирования на «внезапные кибератаки».

Отдельно следует выделить, что, предположительно, благодаря двум основным факторам: решительным действиям руководящего состава Коммунистической партии Китая (КПК) и особенностям китайской правовой системы, КНР делает достаточно серьёзные шаги для победы в конкурентной борьбе за получения статуса государства с наиболее развитым нормативно-правовым регулированием ИИ. В Китае действует принцип коллективной ответственности, применение которого в регулировании ИИ с достаточно высокой долей вероятности, воспринимается обществом в качестве естественного процесса. Так, в Поднебесной с 2022 года на базе Управления по делам киберпространства КНР (**国家互**联网信息办公室) на всеобщее обсуждение вынесен проект «Положения об управлении дипфейками» (**互**联

网信息服务深度合成管理规定) [3], по которому, в случае правонарушения, большая часть ответственности переноситься на поставщика услуг ИИ, а параллельно «в режиме реального времени» возникают первые эпизоды, когда к распространителям дипфейков применяются санкции со стороны сетевой полиции (网络警察). Подобное положение дел может позволить стать КНР «законодательницей мод» в данном направлении с потенциалом на распространения собственной модели на другие страны. Более того, устоявшаяся система правового регулирования ИИ может способствовать росту экспорта соответствующих продуктов от китайских производителей, например, странам-партнёрам, в рамках инициативы «Цифровой шёлковый путь».

Параллельно с 2017 года в Китае реализуется «План развития искусственного интеллекта следующего поколения» (新一代人工智能发展规划) [1], который фактически выступает в качестве фактора, стимулирующего промышленное развитие с применением технологий ИИ в Китае. С помощью указанной внутренней политики, китайские власти потенциально могут повысить уровень национальной и информационной безопасности как за счёт более эффективной системы регулирования, так и с помощью использования технологий ИИ в усовершенствовании критической инфраструктуры [2], а также при работе военных и силовых структур. Спрос на внутреннем рынке на продукты, связанные с ИИ, также может повысится по причине увеличения уровня корпоративного доверия к соответствующим технологиям среди китайских граждан.

Заключение. Глобальные вызовы и угрозы в КНР, в частности нормативно-правовое регулирование ИИ и борьба с внезапными кибератаками (突发性网络攻击, sudden cyber attack), признаются на высшем партийном уровне, где происходит разработка национальных стратегий по

противодействию угрозам в информационном пространстве. При этом современные плановые и нормативно-правовые документы свидетельствуют о намерении китайского руководства не только обеспечить национальную безопасность, но и стимулировать внутренний рынок, а также упрочить позиции на международном уровне в процессе реализации определённых направлений цифрового развития страны. В будущем китайский подход может стать решающим в становлении КНР в качестве мирового лидера в информационном пространстве.

Список источников и литературы:

1. 国务院却发《新一代人工智能发展规划》(Госсовет опубликовал «План развития искусственного интеллекта следующего поколения») [Electronic resource] // 新华社 (Агентство Синьхуа) — URL: https://baike.baidu.com/reference/22036716/475aVSLX5I8spJvSGGHMyw8mvoxctVt_Glu5CFwg0c28t0ivPCaMbfjhNwFj6JCrHppJRq0DPztfj2xdGckvvw4ubLMxtlRcnCXolzuhPnzOT6ye (Дата обращения: 11.04.2023).
2. 科技部启动"人工智能驱动的科学研究"专项部署工作 (Министерство науки и технологий начинает развертывание специального проекта «Научные исследования на основе искусственного интеллекта») [Electronic resource] // xiongan.gov.cn (официальный сайт муниципального правительственного учреждения КНР) — URL: http://www.xiongan.gov.cn/2023-03/28/c_1211899396.htm (Дата обращения: 16.04.2023).
3. 《互联网信息服务深度合成管理规定（征求意见稿）》 («Положение об управлении дипфейками (проект для публичного обсуждения)») [Electronic resource] // cac.gov.cn (официальный Управления по делам киберпространства КНР) — URL: http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm (Дата обращения: 13.04.2023).

4. «十四五» 国家信息化规划 (XIV пятилетний план. Национальная информатизация) [Electronic resource] // 中华人民共和国国家互联网信息办公室 (официальный сайт Администрации по киберпространству КНР) — URL: http://www.cac.gov.cn/2021-12/27/c_1642205314518676.htm (Дата обращения: 19.03.2023).

5. 中共中央 国务院印发《数字中国建设整体布局规划》(ЦК КПК совместно с Госсоветом выпустили «Всесторонний план построения цифрового Китая») [Electronic resource] // 新华社 (Агенство Синьхуа) — URL: http://www.gov.cn/zhengce/2023-02/27/content_5743484.htm (Дата обращения: 19.03.2023).

6. 徐亮. 网络安全面临的新挑战和应对策略 //网络安全技术与应用. – 2021. – С. 148-149.

7. 肖晨卉. 信息时代 “突发性网络攻击” 的安全挑战与应对 //情报杂志. – 2021. – С. 74-79.

Фроловская Виктория Дмитриевна
бакалавр,
Санкт-Петербургский государственный университет,
факультет международных отношений
E-mail: vika.frolovskaya@bk.ru

АНАЛИЗ ВЫЗОВОВ И УГРОЗ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЯПОНИИ И РОССИИ

Аннотация. *Данное исследование ставит своей целью сравнить опыт использования информационных технологий в государственном управлении в России и Японии и выявить общие проблемы, связанные с информационной безопасностью в этих странах. В работе применяются методы сравнительного анализа, «кейс-стади» и анализа документов. В результате исследования выявляются три общие угрозы: киберпреступность, технические сбои и внутренняя угроза (человеческий фактор). Исследование подчеркивает необходимость правового регулирования и защиты информационной безопасности при использовании информационных технологий в государственном управлении.*

Ключевые слова: *информационная безопасность, информационно-коммуникационные технологии, Доктрина информационной безопасности Российской Федерации, информационное право Японии, раскрытие данных, киберпреступность, информационные технологии в государственном управлении, государственная тайна*.

Введение. В современном мире большое значение приобрел вопрос использования информационных технологий в управлении государственными и административными данными. С одной стороны, такие ресурсы, как электронное правительство, позволяют легче и быстрее предоставлять гражданам доступ к информации, что обеспечивает прозрачность в деятельности государственных органов, поддерживает гражданскую

инициативу, помогает противодействовать коррупции [12]. Тем не менее, использование информационных технологий сопряжено с риском: они не только способствуют прозрачности и подотчетности, но и могут подвергнуть угрозе государственную тайну и данные, связанные с национальной безопасностью. Таким образом, актуальность данного исследования обосновывается необходимостью изучения вызовов и угроз в обеспечении безопасности при использовании информационно-коммуникационных технологий (ИКТ) в государственном управлении.

Что касается научной разработанности данной темы, основные отечественные исследования в сфере информационной безопасности относятся к анализу правового регулирования информационной безопасности в России и в мире. Данные вопросы рассматривают Капустин А.Я. [5], Зиновьева Е.С. [3], Ромашкина Н.П., Стефанович Д.В. [8] и другие авторы.

В рамках данного исследования сравнивается опыт использования ИКТ в России и Японии как в нормативном, так и в прикладном аспекте, а также проводится поиск ответа на вопрос, какие общие проблемы в информационной безопасности испытывают указанные страны. Обе страны находятся на высоком уровне развития интеграции ИКТ в государственное управление: они входят группу «Очень высокий Индекс развития электронного правительства» (Very High EGDI), согласно Индексу развития электронного правительства (E-Government Development Index) [13], – при этом они имеют некоторые различия в своем политическом устройстве. Основными методами, помимо сравнительного анализа, являются «кейс-стади» и метод анализа документов, использовавшиеся для сбора и интерпретации информации по теме.

В рамках проведенного исследования были выделены ряд угроз и проблем в информационной безопасности, которые оказались общими для указанных стран: распространение киберпреступности, технические сбои в работе ИКТ и внутренний фактор.

Киберпреступность. Внедрение сервисов электронного правительства и новых технологий может нести в себе угрозу информационной безопасности.

Как и любая другая система, оно не является идеально защищенным от различных видов угроз и преступности в ИКТ-среде. Так, киберпреступность включает в себя любые противоправные действия, которые осуществляются с использованием информационных технологий и сетей.

Как отмечают в своей работе Атнашев В. Р. и Яхъеева С. Н. [1], понятие киберпреступности пока точно не определено, однако есть ряд признаков ее характеризующих, среди которых транспарентный характер, низкий уровень раскрываемости и возможность нанесения большого материального ущерба. Атаки в ИКТ-среде, в свою очередь, являются формой киберпреступности, которая осуществляется с целью нарушения информационной безопасности, нанесения ущерба или хищения конфиденциальных данных.

Согласно исследованию Сергеевой С.Л. и Денисова А.С., угрозу безопасности усугубляет использование цифровых технологий, так как рост числа цифровых соединений приводит к сложностям в обеспечении защиты. Это сказывается на хранении и безопасности использования огромного количества как персональных данных, которые создаются и отправляются в рамках реализации государственных услуг, так и государственно важной информации [9]. Особенно трудно обеспечить безопасность данных в условиях, когда Интернет-провайдеры и поставщики оборудования являются частными компаниями.

Широко известны в России атаки на серверы Центральной избирательной комиссии в 2020 году, что создавало угрозу эффективному проведению голосования по поправкам к Конституции [6]. Проблему киберпреступности и атак на государственную инфраструктуру также разделяет Япония: в 2016 году была обнаружена атака на информационно-коммуникационную инфраструктуру Японской космической исследовательской лаборатории JAXA [14]. Злоумышленники получили доступ к конфиденциальной информации о космических программах Японии.

Технические сбои. Помимо умышленного действия, направленного против информационной безопасности государства, широкое применение

информационных технологий может вызвать и другие угрозы. Одна их них связана с техническими сбоями и отказами в системах ИКТ, так как серверы, базы данных, программное обеспечение и другие инструменты могут стать объектом сбоев. Технические сбои могут быть вызваны различными причинами, включая программные ошибки, аппаратные сбои, ошибки в конфигурации системы, неправильную эксплуатацию и другие факторы. В случае сбоя возможны серьезные последствия, включая потерю данных, нарушение работы сервисов и проблемы с обслуживанием пользователей. Они могут привести к потере данных, затруднить доступ к информации и привести к приостановке работы государственных организаций [11]. Одним из способов снижения риска возникновения технических сбоев в электронном правительстве является использование соответствующих мер безопасности и резервных копий, а также обеспечение регулярного обновления и тестирования системы. Это позволяет уменьшить вероятность возникновения проблем и быстро восстановить работоспособность системы в случае сбоя, однако не защищает полностью от ошибок работы системы.

Внутренняя угроза. Третьим же аспектом является внутренняя угроза, или же иначе человеческий фактор. Внутренние пользователи, а именно сотрудники государственных организаций, могут являться источником угрозы для информационной безопасности как намеренно, так и по случайности. Электронное правительство, предоставляя возможности быстро распространять информацию широкому кругу лиц, усугубляет ущерб, который может быть нанесен утечкой данных, вызванной человеческим фактором. К человеческим факторам относятся, например, ошибки ввода данных, отсутствие контроля и мониторинга за действиями персонала, а также неправильное использование паролей и других средств идентификации. Кроме того, работники и гражданские служащие могут стать жертвой социальной инженерии или фишинговых атак, что может привести к различным формам киберпреступности, таким как взлом систем или утечка конфиденциальных данных. Например, в России за 2022 год отмечается рост утечек персональных

данных россиян и другой информации. Одними из причин этому, помимо интенсификации атак на информационно-коммуникационную инфраструктуру государственных и прочих ресурсов, называется человеческий фактор или активность в торговле персональными данными [7].

Необходимо отметить, что данная угроза является продолжением проблемы из «офлайн мира». Так, и в России, и в Японии существуют законодательные акты, устанавливающие ответственности за разглашение информации, относящейся к государственной тайне или иной информации, имеющей национальное значение (Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 [2] и Закон о защите особых секретов (Act on the Protection of Specially Designated Secrets)（Act No. 108 of 2013) [10] соответственно). Тем не менее, применение законодательства в данной сфере имеет свои особенности. Так, инцидент, опубликованный Асахи Симбун (Asahi Shinbun) в декабре 2022 года, когда капитан японских морских сил самообороны был уволен за утечку государственных секретов своему бывшему начальнику, обнаруживает недостаточную защиты государственных секретов и пробелы в информационном законодательстве Японии [15]. В российской практике также известны случаи разглашения секретных сведений: в 2020 году капитана ФСБ условно осудили за «пробивку» абонентов сотовых сетей [4]. Данные примеры наглядно показывают роль человеческого фактора в вопросах информационной безопасности.

Заключение. Внедрение новых технологий в работу органов публичной власти имеет большое количество преимуществ. Так, электронные порталы позволяют получить доступ к информации быстро и без необходимости подавать официальный запрос. С помощью Интернета и электронных сервисов граждане могут получить доступ к необходимой информации и документам в любое время и из любой точки мира, где есть доступ к сети. Между тем, широкое использование ИКТ ведет к появлению новых и интенсификации уже существующих проблем при работе с информации.

На основе проведенного сравнения опыта Японии и России в сфере использования новых технологий в государственном управлении и работе с информацией можно прийти к выводам, что у стран существуют общие проблемы и угрозы. Более того, они связаны как с техническим (инфраструктурным) аспектом внедрения информационных технологий, так и с правовым регулированием работы с информацией и ее защиты. Данные проблемы в некоторой степени обусловлены дефектами информационного права и предстают развитием проблем из «офлайн-среды». Такие угрозы, как киберпреступность, технические сбои в работе техники и человеческий фактор могут вести к нарушению как национальной безопасности, так и прав граждан как пользователей данных технологий на конфиденциальность и защиту персональных данных.

Список источников и литературы:

1. Атнашев В.Р., Яхъеева С.Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. №3 (29)

2. Закон РФ от 21.07.1993 N 5485-1 (ред. от 05.12.2022) "О государственной тайне" // Консультант.плюс [Электронный ресурс] (URL: https://www.consultant.ru/document/cons_doc_LAW_2481/b6a297f676cd64a5eea867c45fb375fcb1dee3a5/ (Дата обращения: 02.05.2023)

3. Зиновьева Е.С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности // Вестник МГИМО. 2014. №6 (39).

4. Капитан ФСБ семь раз разгласила гостайну [Электронный ресурс] // Коммерсантъ, 09 июля 2020. URL: https://www.kommersant.ru/doc/4408484 (Дата обращения: 11.05.2023).

5. Капустин Ф.А. Информационная безопасность и защита информации в современном обществе // Актуальные проблемы авиации и космонавтики. 2016. №12.

6. Кибератаки в ходе голосования по поправкам совершались из США и стран СНГ // РБК. 07 сентября 2020 [Электронный ресурс] (URL: https://www.rbc.ru/rbcfreenews/5f5635ad9a79475cc99003be (Дата обращения: 12.05.2023)

7. Названы главные причины утечек личных данных россиян [Электронный ресурс] // Lenta.ru, 14.06.2022. URL: https://lenta.ru/news/2022/06/14/leaks/ (Дата обращения: 11.05.2023).

8. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. №5 (39).

9. Сергеева С.Л., Денисов А.С. Электронное правительство на пути к созданию ответственного и эффективного государственного управления // Вестник РУДН. Серия: Политология. 2019. №3.

10. Act on the Protection of Specially Designated Secrets（Act No. 108 of 2013) (URL: https://www.japaneselawtranslation.go.jp/en/laws/view/2543/en#je_apxt1 (Дата обращения: 15.03.2023)

11. Alfredo M. Ronchi. e-Democracy Toward a New Model of (Inter)active Society. // eBook, 2019

12. Bolgov R. and Filatova O. 2022. ICT support of Open Budget as a tool to fight corruption: cases of EAEU countries. In Central and Eastern European eDem and eGov Days (CEEeGov), 2022, Budapest, Hungary. 5 pages.

13. E-Government Development Index. Division for Public Institutions and Digital Government of the United Nations [Электронный ресурс] (URL: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index (Дата обращения: 05.05.2023)

14. Japan aerospace cyberattacks show link to Chinese military: police // Nikkei Asia. December 07, 2021 [Электронный ресурс] (URL: https://asia.nikkei.com/Business/Technology/Japan-aerospace-cyberattacks-show-link-to-Chinese-military-police (Дата обращения: 12.05.2023)

15. MSDF captain dismissed over leak of state secrets to ex-boss, The Asahi Shimbun, December 26, 2022 (URL: https://www.asahi.com/ajw/articles/14802409 (Дата обращения: 15.03.2023)

Чернобривченко Анастасия Олеговна
бакалавр 4 курса
факультета международных отношений,
Дипломатическая академия МИД России
E-mail: chernobrivchenko.ana@yandex.ru

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: ВЫЗОВЫ И УГРОЗЫ

Аннотация. *В работе рассмотрены основы международного сотрудничества в сфере защиты персональных данных на примере ОЭСР и Совета Европы, организаций, инициировавших взаимодействие государств в данной сфере. Проведен обзор деятельности ООН в области защиты персональных данных и международной информационной безопасности в целом. Кратко выделены основные вызовы и угрозы для дальнейшего развития сотрудничества в рассматриваемой сфере, особенно на универсальном уровне.*

Ключевые слова: *защита персональных данных, международная информационная безопасность, ОЭСР, Совет Европы, Рабочая группа открытого состава ООН.*

При изучении персональных данных в контексте международной информационной безопасности (МИБ) необходимо учитывать, что потребность в международном сотрудничестве в целях их защиты возникла практически сразу после принятия первых национальных законов и даже раньше, чем страны осознали необходимость создания единой системы информационной безопасности. Это было связано со стремительным развитием технологий передачи данных и их активного внедрения, прежде всего, в сферу экономики, где они позволяли оптимизировать производственные процессы и повышать прибыль.

Первой организацией, озаботившейся проблемой регулирования вопросов, связанных с защитой персональных данных была Организация экономического сотрудничества и развития (ОЭСР). Уже

в 1978 г. страны-члены создали экспертную группу [8] для разработки принципов обеспечения неприкосновенности частной жизни при трансграничном обмене данными. Как отмечают представители организации, на этот шаг их подтолкнула необходимость создания условий беспрепятственной трансграничной передачи персональных данных [16] для обеспечения непрерывности экономических процессов. Фактически государства стремились создать основу для согласования национальных законов в данной области, чтобы избежать негативного влияния на мировую экономику. Итогом работы к 1980 г. стало принятие «Рекомендаций Совета относительно руководящих принципов, регулирующих защиту частной жизни и трансграничные потоки персональных данных». В этом документе были закреплены положения, которые стали фактически аксиомами в сфере защиты персональных данных. К ним, например, относятся сбор и обработка данных с согласия субъекта и только с четко определёнными целями, принципы обеспечения безопасности, открытости, участия субъекта в процессе использования его данных, максимально возможной свободе трансграничной передачи данных и др. [16] В 2013 г. данный документ был частично переработан, но не изменен целиком, что свидетельствует об актуальности и универсальности его положений.

Стоит подчеркнуть, что сформулированные ОЭСР принципы приняты к использованию во многих государствах мира, однако разные страны трактуют и применяют их по-разному [4]. Это свидетельствует о том, что, несмотря на важную роль документов ОЭСР в развитии области защиты персональных данных, они не способны стать основой для создания международной системы сотрудничества в данной сфере.

Примечательно, что в 2021 г. ОЭСР приняла «Рекомендации Совета по расширению доступа к данным и обмена ими» [17], основной целью которых является создание условий еще более свободного обращения данными для развития ИИ, Интернета вещей и других технологий, основанных на данных. В этом документе отмечается наличие угроз использования данных, в том

числе персональных, для совершенно разных сфер общественной жизни, включая национальную безопасность. При этом анализ отдельных проблем и возможных способов их решения не проводится. Организация, наоборот, вновь акцентирует внимание на мерах, обеспечивающих минимальные гарантии защиты данных, еще более открыто заявляя, что они имеют большую ценность, когда используются как общественное благо. Дальнейшее использование данного принципа в международном сотрудничестве в сфере защиты персональных данных создает реальную угрозу частной жизни людей по всему миру

Вслед за ОЭСР сотрудничество в области защиты персональных данных начали страны-члены Совета Европы. В 1981 г. была выпущена уже упомянутая ранее Конвенция №108. Она стала первым юридически обязывающим документом в сфере защиты персональных данных. В 2001 г. был принят дополнительный протокол, который дополнил раздел про трансграничную передачу данных положениями о взаимодействии со сторонами, не являющимися подписантами данной конвенции, и обязал государства-члены создавать специальные органы по надзору за защитой данных [14]. В 2018 г. Конвенция №108 была значительно переработана. Граждане получили новые права для управления своими данными, кроме того, был расширен перечень данных, относящихся к списку «чувствительных» и требующих дополнительной защиты [15].

Помимо правовой работы Совет Европы занимается популяризацией проблемы защиты персональных данных: реализуются проекты по помощи разным государствам в развитии данной области, регулярно публикуются различные отчеты и исследования по этой тематике, в разных регионах мира проводятся конференции по персональным данным. Так, например, в 2019 г. для исследователей и студентов в области защиты данных была учреждена премия Стефано Родота.

Таким образом, в рамках Совета Европы ведется активная работа по развитию института защиты данных в большей степени с точки зрения

обеспечения прав человека. Документы, разработанные еще в самом начале формирования исследуемой проблематики, поступательно дорабатываются с учетом новых факторов, появляющихся в связи с технологическим развитием, хотя этот процесс происходит довольно медленно. При этом значительное внимание уделяется категории «чувствительных данных», а необходимость трансграничной передачи данных не ставится в абсолют: признается возможность ее ограничения в особых случаях.

Отдельное внимание стоит уделить и международному сотрудничеству в сфере МИБ. В отличие от проблематики защиты данных этот вопрос начал фактически сразу прорабатываться на глобальном уровне. С 1998 г. по инициативе Российской Федерации проблема международной информационной безопасности стала постоянной повесткой ООН [9]. Причиной развития сотрудничества стран в сфере МИБ стали опасения, что новые ИКТ могут быть использованы для дестабилизации ситуации на международной арене и нарушения безопасности государств. Государства признали опасность использования современных технологий в так называемой «триаде» угроз: террористической и преступной деятельности, а также в военно-политическом противостоянии [3]. Они приняли решение совместно прорабатывать существующие и потенциальные угрозы и поставили перед собой цель разработать единый документ, который бы позволил обеспечить МИБ.

Изначально работа по достижению поставленных задач была возложена на Группу правительственных экспертов [10], механизм, в котором принимали участие только ограниченное количество стран, число которых варьировалось от 15 до 25. Позднее, благодаря осознанию необходимости обеспечения участия в работе по обеспечению МИБ всех стран-членов, а также негосударственных акторов, было принято решение о создании Рабочей группы открытого состава (РГОС) ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ [1]. Теперь оба формата работают параллельно.

Несмотря на то, что международное сообщество признает предотвращение угроз в сфере ИКТ невозможным без совместной работы, на данный момент существуют проблемы, препятствующие сотрудничеству в деле обеспечения МИБ и создания доступной и безопасной ИКТ-среды по всему миру.

До сих пор государства и негосударственные акторы не могут прийти к согласию о том, какую терминологию следует использовать для максимально полного охвата всей проблематики МИБ. В основном страны придерживаются двух позиций. С одной стороны, страны Запада предлагают термин «кибербезопасность», стремясь подчеркнуть, что управление ИКТ должно быть связано исключительно с технологическими аспектами, а также вывести за рамки сотрудничества проблемы проведения военных операций в киберпространстве. С другой стороны, Россия и ее сторонники настаивают на использовании понятия «международная информационная безопасность», которое включает в себя не только вопросы нормального функционирования ИКТ, но и социопсихологические и политико-идеологические проблемы, возникающие в ходе их использования. В качестве оптимального для всех сторон варианта в ООН используют формулировку «безопасность в сфере использования ИКТ и самих ИКТ» [3], что позволяет продолжать сотрудничество в данной сфере. Между тем это никак не решает проблему разницы подходов к обеспечению МИБ. Нет окончательного согласия ни по тому, что именно надо регулировать в ИКТ, ни какие существуют угрозы, ни кто должен участвовать в этом регулировании, никаким образом это должно быть реализовано и с помощью каких механизмов международного сообщества. И хотя сама природа цифровой среды подсказывает, что ни одно государство не может обладать абсолютным превосходством в ней, по-прежнему окончательно не решен вопрос, как реализовать государственный суверенитет в информационном пространстве [13]. Раскол можно проследить также по вопросам применимости к информационной сфере международного права в целом [5] и отдельных его отраслей в частности, например,

большинство разногласий возникают относительно международного гуманитарного права и международного права прав человека [3].

Среди других проблем международного сотрудничества в сфере ИКТ выделяются недостаточно высокая скорость переговорного процесса и нежелание «стейкхолдеров» идти навстречу друг другу при обсуждении ключевых моментов взаимодействия и стремление использовать возможности в своих интересах.

Несмотря на наличие достаточно широкого круга вопросов, все еще требующих решения, нельзя полагать, что существующие форматы работы оказываются неэффективными. На данный момент уже разработаны нормы ответственного поведения государств в ИКТ-среде, которые страны договорились дополнять по мере необходимости. В декабре 2022 г. было согласовано создание реестров контактных пунктов для противодействия инцидентам в сфере ИКТ и оперативной ликвидации последствий [2]. Наконец, к 2024 г. страны готовятся представить «Конвенцию по противодействию использованию информационно-коммуникационных технологий в преступных целях» [6], которая может стать первым юридически обязательным документом по борьбе с преступностью в ИКТ-среде. Интересно, что в российском проекте Конвенции, представленном на рассмотрение еще в 2021 г., уделяется значительное внимание защите «цифровой информации» и информации, передаваемой с использованием ИКТ [7]. Кроме того, в нем содержится положение о праве государства-участника признать преступным любое другое деяние, не указанное в Конвенции в случае, если оно совершено с использованием ИКТ и принесло значительный вред. Принятие подобных положений в итоговой конвенции при более детальном анализе угроз, связанных со злонамеренным использованием персональных данных, может сделать этот документ достаточно эффективным с точки зрения не только защиты прав человека в цифровой среде, но и в рамках концепции государственного суверенитета и обеспечения безопасности.

Если говорить о мерах, предпринимаемых в ООН в целях защиты персональных данных, то крайне важно обратить внимание на учрежденный в 2015 г. мандат Специального докладчика по вопросу о праве на неприкосновенность частной жизни, который, в том числе занимается изучением влияния на права человека таких проблем, как массовое слежение, использование и хранение личных данных, криминалистические базы данных ДНК, открытые данные и большие данные. Кроме этого, приняты «Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера» [11], а также ряд резолюций, осуждающих массовую слежку за населением и анализирующих ее влияние на функционирование общества [15]. Тем не менее какой-либо целенаправленной работы государств по проработке вопросов права на защиту персональных данных и угроз, связанных с их ненадлежащим использованием, не ведется. Более того, в официальных документах ООН это право никак не закреплено и в рамках организации рассматривается исключительно как часть частной жизни («privacy»). Вероятно, это связано с расхождением позиций различных государства о необходимости выделения его в самостоятельную категорию.

В целом на данный момент практически все международные организации так или иначе уделяют внимание МИБ, чего нельзя сказать о проблематике защиты персональных данных. Между тем нельзя утверждать, что этот вопрос остается за рамками интересов международного сообщества. Уже более 40 лет защита персональных данных является отдельным направлением работы СЕ и ОСЭР. Позднее это направление вошло в повестку дня и некоторых других международных площадок, например, ЕС, СНГ и др. А страны Иберо-Америки даже создали отдельную региональную организацию по защите данных [12], «Ибероамериканская сеть защиты данных» (Red Iberoamericana de Protección de Datos – RIPD). Все это в совокупности создает достаточную основу для дальнейшей разработки проблематики защиты персональных данных.

Таким образом, проведенный обзор международного сотрудничества в сфере МИБ и персональных данных показал, что на данный момент эти вопросы активно прорабатываются на различных площадках. При этом государства стремятся следить за тенденциями постоянно развивающихся ИКТ и приводить в соответствие с ними имеющиеся документы для обеспечения более эффективного регулирования, хотя этот процесс и не «успевает» за изменениями в рассматриваемой сфере. На международном уровне в контексте персональных данных в большей степени уделяется внимание именно угрозам, связанным с нарушением прав человека, а особенно права на неприкосновенность частной жизни. При этом вопросы безопасности и суверенитета государств в контексте защиты персональных данных все еще не входят в повестку международных организаций.

Более того, даже на уровне международных организаций просматривается значительное расхождение в подходах к вопросам защиты персональных данных, что может стать одним из основных препятствий для государств в случае расширения сотрудничества в данной сфере.

На универсальном уровне государства пока не пришли к необходимости отдельной работы по защите данных, однако деятельность, которая ведется в сфере МИБ, имеет крайне важное значение и для рассматриваемой области. В частности, разрабатываемая в рамках ООН «Конвенция по противодействию использованию информационно-коммуникационных технологий в преступных целях» может сыграть большую роль в предотвращении злонамеренного использования данных. Однако разрабатываемых универсальных норм может оказаться недостаточно для обеспечения полноценной защиты персональных данных, а предметной работы по этому вопросу на площадке ООН все еще не ведется, хотя эффективное обеспечение защиты персональных данных требует глобальных усилий.

Список источников и литературы:

1. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: доклад Генерального секретаря от 11

декабря 2018 г. A/73/27. [Электронный ресурс] // Организация Объединенных Наций: [сайт]. URL: United Nations Official Document

2. Интервью заместителя Министра иностранных дел Российской Федерации О.В.Сыромолотова МИА «Россия сегодня» в связи с принятием 7 декабря 2022 г. предложенной Россией резолюции ГА ООН по обеспечению международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел Российской Федерации: [сайт]. 10.12.2022. URL: https://www.mid.ru/ru/foreign_policy/news/1842982/

3. Крутских А.В. «Международная информационная безопасность: подходы России»… 48 с.

4. Курбалийя Й. Управление Интернетом / Й. Курбалийя. Координационный центр национального домена сети Интернет. – М., 2016. – С. 331

5. Мартиросян А.Ж. Формирующиеся международное информационное право и система обеспечения международной информационной безопасности: теоретические векторы [*Электронный ресурс*] // Вестник учёных-международников. 2022. № 2 (20). С. 179-188. *URL:* https://www.dipacademy.ru/library/periodical/zhurnal-vestnik-molodykh-uchenykh-i-diplomatov/

6. О второй сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности [Электронный ресурс] // Министерство иностранных дел Российской Федерации: [сайт]. 16.06.2022. URL: https://www.mid.ru/ru/foreign_policy/news/1818160/

7. Проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях от 29.06.2021 [Электронный ресурс] // Организация Объединенных Наций: [сайт]. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

8. Соколова М. Защита персональных данных: международные принципы и стандарты [Электронный ресурс] // ResearchGate: [Сайт]. URL: https://www.researchgate.net/publication/281459857_Zasita_personalnyh_dannyh_mezdunarodnye_principy_i_standarty

9. Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 декабря 1998 г. [Электронный ресурс] // Организация Объединенных Наций: [сайт]. URL: United Nations Official Document

10. Резолюция ГА ООН A/RES/56/19 от 29 ноября 2001 г. [Электронный ресурс] // Организация Объединенных Наций: [сайт]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement

11. Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера A/RES/45/95 от 14 декабря 1990 года [Электронный ресурс] // Организация Объединенных Наций: [сайт]. URL: https://www.un.org/ru/documents/decl_conv/conventions/computerized_data.shtml

12. Шебанова Н. А. Охрана персональных данных: опыт международного регионального сотрудничества [Электронный ресурс] // Международное право и международные организации. 2020. №2. URL: https://cyberleninka.ru/article/n/ohrana-personalnyh-dannyh-opyt-mezhdunarodnogo-regionalnogo-sotrudnichestva

13. Яковенко А.В. Цифровой суверенитет оказался важен в условиях новой идеологической конфронтации [Электронный ресурс] // Russian Council: [сайт]. 2021. URL: https://russiancouncil.ru/analytics-and-comments/comments/tsifrovoy-suverenitet-okazalsya-vazhen-v-usloviyakh-novoy-ideologicheskoy-konfrontatsii/

14. CdE, Protocole additionnel à la Convention pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, STCE nº

181, 2001 [ressource électronique] // Conseil de l'Europe : [site]. URL : https://rm.coe.int/168008062f

15. Manuel de droit européen en matière de protection des données [Texte] / réd. Christos Giakoumopoulos, Giovanni Buttarelli, Michael O'Flaherty. – Luxembourg : Office des publications de l'Union européenne. 2019. P.30.

16. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data as of 23/09/1980 [Electronic
resource] // OECD: [Website]. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188#mainText

17. Recommendation of the Council on Enhancing Access to and Sharing of Data as of 06/10/2021 [Electronic resource] // OECD: [Website]. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463

18. Карпович О.Г. Особенности ведения современных информационных войн в СМИ и сети интернет // Мировая политика. 2017. № 4. С. 64-74.

19. Карпович О.Г. Цветная "революция зонтиков" в Гонконге: начало "китайской весны" // Национальная безопасность / Nota Bene. 2014. № 6 (35). С. 990-996.

20. Информационная безопасность в контексте национальной политики России. Шангараев Р.Н., Дипломатическая академия МИД России. Москва, 2020

21. Современные технологии информационного противоборства в интернет-пространстве. Шангараев Р.Н., Ногмова А.Ш., Дипломатическая академия МИД России, Москва, 2020.

СЕКЦИЯ 4

«МЕЖДУНАРОДНО-ПРАВОВОЕ ИЗМЕРЕНИЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ»

Васильева Анастасия Андреевна
студент-бакалавр
кафедры международного и интеграционного права
Российской академии народного хозяйства и службы при Президенте РФ
E-mail: nast.vasiljva2010@yandex.ru

МЕЖДУНАРОДНО-ПРАВОВЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ НАСИЛИЮ НАД ДЕТЬМИ В КИБЕРПРОСТРАНСТВЕ

Аннотация. *Исследование посвящено анализу правовых систем в сфере противодействия насилию над детьми в Интернете. Были проанализированы законодательства универсального, регионального и национальных уровней. Было предложено создать единый нормативный акт, регламентирующий данную сферу.*

Ключевые слова: *насилие, насилие над детьми, интернет, киберпространство, международное публичное право.*

В наше время киберпространство играет огромную роль в жизни людей, включая и детей. Интернет стал неотъемлемой частью их повседневной жизни: дети общаются со сверстниками, получают образование, развлекаются и находят новых друзей. Однако это пространство также стало местом, где совершаются преступные деяния, в том числе и против детей.

Для написания статьи были использованы следующие методы для достижения поставленных целей и задач: конкретно-исторический, сравнительно-правовой, логический, обобщение и статистический, аналитический.

С момента становления Интернета и его массового использования возникли правонарушения, которые основывались на наивности и доверчивости пользователей, включая детей. Например, преступники могли выманивать деньги, представляясь обеспеченными людьми и обещая вернуть больше. Дети могли использовать свои сбережения в этой схеме и потерять их. В то время как Интернет продолжал развиваться, появились новые виды киберпреступлений, включая груминг и шантаж. Сейчас, когда дети все чаще

имеют доступ в Интернет, повышается риск для несовершеннолетних. Кроме того, не все подростки открыты для общения с родителями, поэтому опекуны не всегда знают, что происходит с их детьми.

Одним из основных инструментов, предназначенных для защиты прав детей в Интернете, является Конвенция ООН о правах ребенка. Однако ряд других международных документов также содержат рекомендации и меры, направленные на борьбу с насилием над детьми в ИКТ-пространстве [4].

Если говорить про универсальный уровень, то здесь достаточно много организаций, занимающихся как раз защитой прав детей в Интернете, например ЮНИСЕФ, МОТ, ВОЗ и так далее [5]. На заседаниях данных организаций происходит обсуждение по безопасному использованию несовершеннолетними сети Интернет. В данном контексте каждое государство инициирует свои индивидуальные меры. На данный момент не существует единого нормативно-правового акта, который бы регулировал данные вопросы комплексно. На региональном уровне тоже существуют некоторые инициативы со стороны отдельных международных организаций. В качестве примера можно привести создание ЕС специальной программы (ENISA), которая как раз и занимается обеспечением безопасности в Интернете, в том числе и безопасности несовершеннолетних [6]. В других региональных организациях, к примеру, в Организации американских государств или Содружестве независимых государств тоже происходит работа над осуществлением мер по защите детей в киберпространстве. Но мне представляется это недостаточным, необходимо, чтобы во всех государствах существовали однотипные меры воздействия на правонарушителей в данной сфере.

В ряде зарубежных стран проблема насилия над детьми в Интернете проработана более глубоко и полно. К примеру, в азиатском регионе разработана целая система по защите несовершеннолетних от пагубного влияния Интернета (существуют приложения, ограничивающие доступ к определенному количеству сайтов, без которых устройство не может быть

продано ребенку или система, распознающая возраст пользователя). Достаточно серьезные ограничения вводятся в Китае: в учебных заведениях запрещены все устройства, имеющие доступ в Интернет, а также если замечено, что ребенок стал зависимым от Интернета, применяются меры по «исправлению» несовершеннолетнего, более того, там запрещено несовершеннолетним играть в компьютерные игры с 22 часов вечера до 8 часов утра [7]. США начали освещать данную проблему еще в 90-е года прошлого века, в связи с появлением Интернета. Нормативно-правовые документы, принятые тогда, до сих пор остаются действующими и актуальными. Что касается Российской Федерации, то у нас существует ряд нормативно-правовых актов, одним из которых является закон «О защите детей от информации, причиняющей вред их здоровью и развитию», также внесены различные поправки в действующие нормативно-правовые акты (например, в Уголовный кодекс). Более того в нашей стране существуют различные фонды, которые занимаются распространением информации о безопасном использовании сети Интернет (ими проводятся всевозможные мероприятия), а также ими разрабатывается системы безопасности для несовершеннолетних. При этом в Российской Федерации достаточно активно развивается законодательство в данной сфере. К примеру, в период написания настоящей исследовательской работы были приняты следующие нормативно-правовые акты: Указ Президента Российской Федерации «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года» [1], Распоряжение Правительства Российской Федерации «Концепция информационной безопасности детей в Российской Федерации» [6].

Подводя итог проведенному исследованию, хотелось бы отметить, что государства пытаются противодействовать насилию над несовершеннолетними в киберпространстве с 1990 годов. В каких-то странах регулирование этой сферы уже сейчас является достаточно жестким (например, Китай, Япония или Южная Корея), а в каких-то странах почти не существует отдельных законов, защищающих детей в Интернете, так как они

являются членами интеграционных объединений, а их законодательство выше национального правового регулирования этих стран (к примеру, Франция, Португалия, Испания, Италия и т. д.). Но несмотря на долгое существование Интернета в целом, а также и проблемы насилия над детьми в киберпространстве, не существует единого нормативно-правового акта, который бы решал все вопросы, возникающие в данной сфере, ни на универсальном, ни на региональном уровнях. Представляется необходимым инициировать процесс разработки такого вида правового регулирования на уровне Организации Объединенных Наций, в котором будут определены все понятия, виды насилия, а также ответственность за нарушение созданных правил. Ограничение доступа детей к Интернету не является правильным решением, поскольку киберпространство представляет собой сложный феномен, обладающий как позитивными, так и негативными сторонами. Несовершеннолетние такие же люди, со своими правами и обязанностями, которых просто нужно защищать чуть более активно из-за их возраста.

Список источников и литературы:

1. Алисиевич Е., Николаев А., Кебурия К. Влияние цифровизации на международные стандарты в области прав человека и обязательства государств по их соблюдению // Международное правосудие. 2021 № 4 (40). С. 57–76.

2. Румянцев П. П. Безопасность детей в сети Интернет: мировая практика // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи: Сборник статей. – Магнитогорск, 2014.

3. ENISA // URL: https://www.enisa.europa.eu/

4. Закон "Закон Китая о защите несовершеннолетних (未成年 人 保护 法)" от 01.06.2021

5. Указ Президента Российской Федерации "Указ Президента РФ от 17 мая 2023 г. № 358 "О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года"" от 17.05.2023 № 358

6. Акт Правительства Российской Федерации "Распоряжение от 28 апреля 2023 г. № 1105-р, Концепция информационной безопасности детей в Российской Федерации" от 28.04.2023 № 1105-р

Жебриков Василий Витальевич
3 курс, специалитет
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
E-mail: iarturian@inbox.ru

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МЕЖДУНАРОДНОГО ПРЕСТУПЛЕНИЯ АГРЕССИИ КАК АКТА, СОВЕРШАЮЩЕГОСЯ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СРЕДЕ

Аннотация. *В настоящей статье в условиях текущего универсально-правового регулирования рассматриваются юридически, значимые и сущностные аспекты квалификации международного преступления агрессии как акта, совершающегося не с характерными для данного вида общественно опасного деяния признаками объективной стороны, выраженной в посягательстве на мир и безопасность посредством применения силовых мер и использовании комплекса конвенциональных вооружений в пределах классической архитектуры театра военных действий (ТВД), состоящего из сухопутного, морского и воздушного пространств, а как особо тяжкого международного деликта, реализующегося в информационно-коммуникационной среде посредством применения электронно-цифровой инфраструктуры.*

Ключевые слова: *информационно-коммуникационные технологии, информационно-коммуникационная среда, преступление агрессии, международное преступление, квалификация, цифровая инфраструктура, международно-правовая ответственность, состав преступления, противоправное деяние.*

В настоящее время особое место в силу неразрешенности проблемы и наличия правового пробела в аспекте теоретико-доктринального рассмотрения занимает дискуссия о допустимости применения нормативных универсальных договорных и иных рекомендательных положений международного уголовного права и права международной безопасности в

вопросе квалификации международного преступления агрессии как акта, совершающегося не с характерными для данного вида общественно опасного деяния признаками объективной стороны, выраженного, в обобщённом смысле, в применении силовых мер или создания соответствующих условий посредством вооружений для посягательства на мир и безопасность, суверенитет и политическую независимость государств, а как особой виртуальной операции с задействованием информационно-коммуникационной среды и в целом потенциала электронно-цифровой инфраструктуры и вычислительно-аппаратных мощностей.

Одним из первоосновных препятствий, связанным с квалификацией конкретных деяний, содержащих юридически определяющие признаки виртуально-цифровой операции как международного преступления агрессии является то, что в настоящее в контексте универсально-правового регулирования и императивных, обязывающих норм, не выработано норм, согласно которым информационно-коммуникационные технологии рассматриваются как оружие (за исключением позиций толкования, принятого в условиях региональных многосторонних соглашений по информационной безопасности, например СНГ,ШОС, НАТО). Это, во-первых, является одним из важнейших, хотя и не необходимых признаков объективной стороны противоправного деяния, имеющего признаки агрессии, согласно Резолюции ГА ООН 3314(ст.2) [1], Уставу ООН(ст.39) [2] и Резолюции RC/Res.6 [3], принятой для целей Римского Статута Международного уголовного суда(далее- Статут МУС) (ст.5) [4].

В связи с противоречием деятельности Международного уголовного суда(далее-МУС) внешнеполитическому курсу и национальным интересам Российской Федерации, принявшей в 2016 году решение не становится участником Статута МУС [5], стоит особо заострить внимание на том, что в рамках данной статьи положения Статута МУС, касающиеся юридически значимых для квалификации признаков составов международных преступлений, рассматриваются вне какой-либо связи с текущим положением

дел в сфере международных отношений и, в частности, с позицией, которую в настоящий момент занимает МУС как участник международных отношений и как субъект международного права, а, в свою очередь, анализируются исключительно как источник права, как совокупность универсально правовых норм о конкретных, зафиксированных составах международных преступлений, имеющих юридически обязывающую силу.

Таким образом, возвращаясь, к обозначенной проблематике, как было упомянуто выше, данный критерий относимости средства совершения общественного опасного акта к комплексу вооружений, хотя и важен, но не исчерпывающ, что прямо констатируется Резолюцией 3314 в виде допустимой возможности у СБ ООН квалифицировать иные действия, не соотносящиеся с альтернативными составами международного преступления агрессии (ст.3), по собственному усмотрению как непосредственное выражение неправомерных актов агрессии (ст.2 и 4), а, потому, даже отсутствие конвенционно-нормативного признания ИКТ как оружия в текущий момент, в целом, не препятствует квалификации операций в ИКТ-среде как умышленно посягающих на международный мир и безопасность, но, в любом случае, оставляет размытым и неоднозначным будущий, перспективный толковательный подход в отсутствии очерченной конструкции преступления [6].

Помимо вышеупомянутой проблемы, которая, в целом и общем, разрешима с учётом имеющихся договорных норм, другим несовершенством технического, неюридического характера является, как правило, анонимность, или, минимум, неопределённость субъектного состава в частности и субъективной стороны в целом международного преступления агрессии, совершающегося в форме цифрового акта. Апеллируя к содержанию Резолюции RC/Res.6, принятой для целей Римского Статута Международного уголовного суда (ст.5), в частности, к п.1 Приложения 1, существенным требованием к лицу, которое будет потенциально нести ответственность за совершение преступления агрессии, являются в общем смысле базовые,

классические критерии дееспособности, или более конкретнее, «возможность фактически осуществлять руководство или контроль за политическими или военными действиями государства». В случае с виртуально-цифровой операцией, несмотря на общепризнанную концепцию международно-правовой (политической и материальной) ответственности государств за деятельность собственных компетентных органов и должностных лиц, исполняющих делегированные публично-властные функции, идентифицировать определенное ответственное уполномоченное лицо или правительственную структуру, беря во внимание специфику самого противоправного акта, реализующегося с использованием обезличенных, штатных программно-технических и компьютерно-электронно-аппаратных средств, представляется, в принципе, крайне затруднительным, а, во многих ситуациях, невозможным. Например, когда речь идёт о применении ИКТ против интересов одного государства юридическими или независимыми физическими (частными) лицами безотносительно фактора участия в этом другого, противоборствующего государства, по просьбе которого такие ИКТ используются. Другими словами, доказать факт заинтересованности государств будет весьма проблематично. Не менее существенным, ввиду вышесказанного, является и то, что, опять же беря в расчёт специфический характер операций в ИКТ-среде, и общие критерии деликтоспособности, установить реальную, обозреваемую связь между последствиями и, собственно, самим актом агрессии, совершенного в виртуальной сфере, а, следовательно, и оценить фактическую степень и характер нанесённого таким виновным посягательством ущерба, создав базовые, необходимые условия для ответственности, является не менее трудоёмким процессом, в некоторых случаях полностью исключающим, в принципе, само по себе событие преступления.

В числе других сложностей, связанных с квалификацией электронных процедур как действий, образующих состав международного преступления агрессии, можно назвать и практическую невозможность определить

классическую для текущего права международной безопасности и международного гуманитарного права архитектуру театра военных действий (ТВД), который, опираясь на наиболее общую точку зрения, представляет из себя сухопутное, морское и воздушное пространство, в то время как ИКТ-среда, несмотря на отсутствие какой-либо понятийно-дефинитивной фиксации, являет собой, опять же с наиболее общераспространённой точки зрения, уникальное виртуально-цифровое измерение без чёткой пространственно-физической, территориально-осязаемой привязки[7].

Заключение. Таким образом, на основе вышеприведённого, учитывая существующие проблемы в универсально-правовом регулировании и специфику рассматриваемого явления, полагается рациональным предложить следующие пути решения проблем:

1) Зафиксировать на уровне внутреннего нормативного содержания Резолюции RC/Res.6 принятой для целей Римского Статута Международного уголовного суда, в частности, для Приложения 1(п.1-2) и Резолюции ГА ООН 3314(ст. 5) новый самостоятельный, автономный, независимый альтернативный состав, образующий, в числе других, международное преступление агрессии, объективная сторона которого будет выражена в применении, использовании или угрозы применения и использования ИКТ и ИКТ-среды (в числе компьютерно-цифровой инфраструктуры, аппаратно-вычислительных мощностей, электронных и программно-технических средств) в качестве средства посягательства на внутренние дела, политическую независимость, территориальную целостность, национальные интересы государств, на международный мир, безопасность и человечность,

2)Взять в качестве материально-правовой позиции, в вопросе привлечения к ответственности, положение (презумпцию) о территориально-юрисдикционном (государственном) факторе привязки (местоположения) средств цифровой инфраструктуры, используемых в целях совершения акта агрессии во избежание потенциальных негативистских толковательных подходов к ИКТ-среде как не имеющей подлинной, реальной связи с

физическим миром, лишающих правоприменителя всех возможных механизмов воздействия, а виновное лицо, собственно, реальной связи между непосредственно ним и последствиями его неправомерных действий и исключающих само по себе «событие преступление». Подобную позицию необходимо избрать и в случае предоставления объектов электронной инфраструктуры со стороны третьих государств, определяя территориально-юрисдикционный измерение (то есть, собственно, их территорию) как первоосновной фактор привлечения к ответственности конкретных уполномоченных лиц, компетентных структур и даже независимых юридических и физических лиц, зарегистрированных на территории этих государств.

Список источников и литературы:

1.Резолюция Генеральной Ассамблеи №3314 от 14 декабря 1974 года [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/aggression.shtml (дата обращения: 22.06.2023).

2. Устав Организации Объединённых Наций [Электронный ресурс]. – Режим доступа: https://www.un.org/ru/about-us/un-charter/full-text (дата обращения: 22.06.2023)

3. Резолюция RC/Res.6, принятая для целей Римского Статута Международного уголовного суда [Электронный ресурс]. – Режим доступа: https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf (дата обращения: 22.06.2023).

4. Римский статут Международного уголовного суда [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/901750575 (дата обращения: 22.06.2023).

5. Заявление МИД России [Электронный ресурс]. – Режим доступа: https://www.mid.ru/ru/press_service/spokesman/official_statement/1538221/ (дата обращения: 22.06.2023).

6. Дылевский И.Н, Комов С.А, Коротков С.В, Родионов С.Н, Полякова Т.А, Федоров А.В. К вопросу о международно-правовой квалификации информационных операций. // Военная мысль. 2008. №2. С.3.

7. Вахитова Гузель Валериевна, Шонин Николай Егорович. Информационные технологии и международное право. // Правовое государство: теория и практика. №1. С. 194.

Мамкин Владислав Юрьевич
студент-магистрант
кафедры информационного права и цифровых технологий
Московского государственного юридического университета
имени Олега Емельяновича Кутафина,
Email: vlad562169@mail.ru

О МЕЖДУНАРОДНОМ КОМПОНЕНТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ – ВОПРОСЫ И ЗАДАЧИ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. *Исследование посвящено вопросам создания и обеспечения информационной безопасности при внедрении искусственного интеллекта (ИИ) как инновационного компонента международных отношений. В новых политических и экономических реалиях специалистами осуществлён призыв к приостановлению экспериментов, связанных с ИИ. В связи с этим автором проанализированы основные угрозы со стороны технологий искусственного интеллекта при обеспечении международной информационной безопасности (МИБ), а также выявлены возможные способы обеспечения безопасности на международном уровне в условиях цифровой синергии.*

Ключевые слова: *международная информационная безопасность, кибербезопасность, информационные угрозы, тактические задачи, интеллектуальная система, правовое регулирование, искусственный интеллект, принципы и нормы права.*

По данным многочисленных аналитиков, ИИ в сравнении с интеллектом людей способен доставлять существенные риски для человечества [2]. Это признано лидирующими лабораториями, проводящими исследования ИИ. Если исходить из данных, указанных в Принципах ИИ Асиломара [10], улучшенный ИИ способен проявлять себя как существенная перемена в истории жизни на планете. Необходимо, чтобы он планировался и руководствовался с определённой осторожностью и компонентами.

К сожалению, такого уровня планирования и управления не происходит, даже несмотря на то, что в последние месяцы лаборатории ИИ оказались вовлеченными в неконтролируемую гонку по разработке и развертыванию все более мощных цифровых умов, которые никто, даже их создатели, не может понять, предсказать или надежно контролировать.

Нынешние модели ИИ в современном мире являются конкурентами для людей при решении определённых целей. Исходя из такого вывода, возникают вопросы, касающиеся правового регулирования. Вынуждены ли мы, люди, допустить машины к заполнению источников информации ложью и агитацией? Обязано ли человечество произвести автоматизацию всех рабочих зон, включая выполняемые? Должны ли люди заниматься развитием нечеловеческого рассудка, потому что в конце он способен преобладать над количеством людей, их хитростью, старением и по итогу заменить людей? Вынуждено ли человечество рисковать утратой контроля над цивилизацией? Эти решения не должны поручаться технологическим руководителям, которые ещё не избраны. Сильные системы ИИ должны создаваться лишь тогда, когда люди убеждены, что их результаты окажутся утвердительными, а их риски станут управляемыми. В зависимости от уровня величины вероятного влияния системы уверенность должна быть удачно аргументирована и возрастать. В недавнем заявлении OpenAL по поводу общих интеллектуальных систем содержится информация о том, что в определённой ситуации может быть важно провести самостоятельную отдельную проверку, прежде чем начать обучать системы будущего, и приложить существенное количество усилий, чтобы договориться ограничить скорость роста вычислений, которые служат для того, чтобы сделать новые модели. Мы поддерживаем указанную точку зрения, как актуальную в данный момент. Так, одно из направлений сегодняшней правовой задачи является юридическое сопровождение призыва всех лабораторий ИИ к немедленному приостановлению, как минимум, на 6 месяцев обучение систем ИИ, более мощных, чем GPT-4. Приостановление должно быть открытым для всех и

поддаваться проверке, добавляя всех основных участников. Если же такая пауза не сможет быть быстро введена, должны вмешаться основные государственные органы для введения ограничения. Лаборатории искусственного интеллекта и суверенные специалисты должны использовать это приостановление в целях коллективной разработки и введения набора общих протоколов защищённости для более полного проектирования и разработки ИИ, за которыми введётся внимательный мониторинг внешними специалистами.

Подобные документы обязаны давать гарантию того, что системы, которые их придерживаются, являются безопасными вне любых здравых сомнений. На наш взгляд, такое действие не является основанием для временного прекращения развития искусственных интеллектуальных систем в целом, а лишь заключается в сделанном шаге назад от непредсказуемых моделей с новыми возможностями, которые могут создать существенную опасность.

Анализ и разработки в сфере интеллектуальных систем должны быть перенаправлены на то, чтобы создать новейшие системы наиболее точными, надёжными, слаженными, благонамеренными, доверительными для общества.

Одновременно создатели ИИ обязаны взаимодействовать с политиками для того, чтобы существенно увеличить скорость разработки безопасных систем регулирования ИИ.

Разработчикам необходимо хотя бы задействовать новые и дееспособные регулирующие органы, которые занимаются ИИ, надзором и отслеживанием систем ИИ с повышенной работоспособностью, результативностью и больших пулов расчётных возможностей, системы возникновения и водяных знаков. Именно последние помогают делать отличие настоящего от синтетического и следить за утечкой моделей. Также необходимо подключить надёжную экосистему аудита и сертификации, предусмотреть ответственность за вред, который причиняется ИИ, обеспечить денежными и иными средствами со стороны государства на технические исследования в области защищённости интеллектуальных систем, снабдить необходимыми ресурсами институты для

борьбы с драматическими финансовыми и политическими неблагоприятными изменениями, которые может вызвать ИИ [14].

Хотелось бы отметить, что при повсеместном внедрении цифровых технологий в разные сферы жизни, появляются новые опасности в области информатизации, носящие масштабный характер [6]. Для того что бы создать результативную борьбу вызовам в области информатизации нужен специальный орган на международном уровне в сфере международной информационной безопасности. Исходя из слов министра иностранных дел Российской Федерации С.В. Лаврова, Россия является очередным членом объединения действий стран для более результативного разрешения стоящей проблемы [7].

Основную функцию в механизме содержания МИБ выполняет право. Проблемы создания системы международно-правовых норм, которая бы регулировала информационную безопасность на международном уровне, обладают междисциплинарным свойством. Они содержат в себе «перечень теоретических вопросов по праву для использования норм, правил и принципов добросовестного поведения стран, которые нужны для оказания содействия открытой, защищенной, устойчивой, доступной и спокойной информационно-коммуникационной среды» [9]. Оборона независимости стран в информационной среде выступает государственным интересом в данной области [1]. Существенное значение в обозначенной сфере правового контроля оказывают нормы международного и информационного права.

Если исходить из Указа Президента РФ от 12 апреля 2021 г. № 213, то международной информационной безопасностью является «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» [12].

Специалисты МГИМО отмечают, что международная информационная безопасность предполагает собой наличие не только политико-

идеологических опасностей в этой сфере, но и технических. Это явление не взаимосвязано с представлением Запада о цифровой безопасности, которое устанавливает свою заинтересованность на технологическом распознавании информационной опасности [5]. Такая точка зрения показывает мнение большого количества экспертов из России в сфере информационного права, выделяющие модули защищённости сведений и информационно-психологической защищённости в составляющей предмета правового снабжения информационной защищённости.

В Основах государственной политики целью Российской Федерации в сфере МИБ является помощь в налаживании международно-правового режима, в результате чего появляются условия для недопущения и устранения межнациональных споров в мировом информационном пространстве, а также для развития, учитывая национальные интересы Российской Федерации систем снабжения МИБ. Результат данной цели создаётся через решение задач по развитию международной договоренности России на мировом и других уровнях по вопросам возникновения новых информационных угроз.

Основными тактическими задачами РФ в рассматриваемой области являются:

– развитие на международной арене российских подходов для развития системы снабжения МИБ и российских инициатив в данной сфере;

– деятельность, направленная на формирование международно-правовых механизмов недопущения конфликтов государств в глобальном информационном пространстве;

– организация межведомственного взаимодействия при реализации государственной политики в области МИБ.

В Указе содержатся основы для реализации политики РФ в сфере МИБ на платформе системного развития правового обеспечения МИБ.

Стоит отметить, что степень развития правовых основ в области МИБ, не зависимо от её особого значения, остается явно низким. В настоящее время до сих пор не принят международный НПА на универсальном уровне, который

излагал бы эту область отношений. Столкновения интересов мировых держав до сих пор выступают основной преградой для развития международного права в сфере МИБ.

Сложившиеся ситуация не означает, что в нынешнее время возник вакуум в регулировании международно-правовых вопросов безопасности в сфере информационных технологий.

1. Если начать с конца 90-х годов Генеральной Ассамблеей ООН был принят ряд НПА «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Именно в них определены главные опасности МИБ и этапы развития международного сотрудничества государств в данной сфере. Тем не менее, данные резолюции не носят юридически обязательного характера [8];

2. В 2000-е гг. было принято несколько международных документов политического характера, касающиеся развития информационного общества, в которых существенное внимание уделялось вопросам защищённости использования информационно-коммуникационных технологий (ИКТ).

3. Противодействие другим категориям опасностей МИБ частично трактуются в универсальных и территориальных международных документах в сфере СМИ и Интернета, борьбы с преступностью и терроризмом.

4. ООН утвердила необязательные и основанные на добровольных началах нормы добросовестного поведения стран в информационной среде.

5. В сфере МИБ принят ряд обязательных для исполнения международных договоров на двустороннем и региональном уровне.

За последние несколько лет значительно отразились существенные причины для введения универсального международного договора в сфере обеспечения безопасности в цифровой среде.

Так, в 2019 году в результате активных действий нашего государства учрежден специальный комитет ООН для того, чтобы подготовить всеобъемлющей международной конвенции в этой сфере. В 2021 г. Россия внесла в такой комитет проект Конвенции ООН о противодействии

использованию информационно-коммуникационных технологий в преступных целях [4]. Деятельность над таким проектом должны будут завершить в 2023 г.

Тем не менее, перечень достижений в сфере правового регулирования других аспектов и направлений МИБ ни в какой мере не производят отмену нужды принятия универсального НПА в сфере МИБ, так как такой документ будет юридически значимым, необходимым и носить императивный характер. В таком НПА должны содержаться меры по устранению использования ИКТ с целью нарушения мира и защищённости и поддержке работы стран в ИКТ-среде, способствующей экономическому и социальному развитию государств на основе исполнения принципов и законов международного права.

Из-за возникших трудностей развития определённых целей и в ситуациях происходящих серьёзных изменений возможности принятия в ближайшие годы общего для всех международного договора в области МИБ оказываются все более неясными. Такое явление происходит из-за агрессивной позиции держав с Запада, которые раньше всяким образом устанавливали блокировку инициатив со стороны России, а в последнее время заняли прямо и открыто недоброжелательную позицию в отношении России. Исходя из мнения председателя Конституционного Суда РФ, страны запада начали системную войну против России из-за чего людям приходится жить в ситуации частичной международной обособленности [3].

Также следовало бы сказать о том, что в ситуации происходящего информационного противоборства против России преимущественную роль имеет объединение сил для совместного обеспечения государственной и международной информационной безопасности с нашим соседним стратегическим мобилизационным товарищем – Республикой Беларусь. Миссия обеспечения защиты сведений информационных средств Союзного государства находится в Приоритетных направлениях и первоочередных задачах дальнейшего развития союзного государства на 2018 – 2022 годы [11].

В наше время предложения для более гуманного и обоснованного развития правового обеспечения информационной защищённости Союзного государства на основе наилучших методов и правовых устройств необходимы для того, чтобы регулировать отношений в такой регулярно изменяемой области. Большинство ученых придерживаются мнения о том, что в эпоху цифровизации средства правового регулирования должны быть очень податливыми, подстраиваемые, чтобы должны образом снабжать оперативную выработку системы методов и средств реакции на новые опасности и обращения [13].

Заключение. На основе проведенного анализа можно сделать вывод о том, что система юридического обеспечения МИБ недостаточна и фрагментарна. Существующие международные договоры в области противодействия киберугрозам только отчасти касаются вопросов безопасного применения ИКТ. До настоящего периода нет основного, всеобщего международного договора в сфере МИБ, хотя существует положительный опыт разработки аналогичных актов в рамках региональных компаний с участием РФ (ОДКБ, ШОС). На наш взгляд, необходим рост инициативы России по принятию Конвенции об обеспечении МИБ. Вместе с этим нужно нацелить силы на развитии юридического регулирования МИБ в рамках региональных международных компаний с участием РФ, включая двусторонний уровень.

Список источников и литературы:

1. Бойко С. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. 2018. № 11. С. 26; Холодная Е.В. О правовых задачах обеспечения кибербезопасности: перспективы развития // В сборнике: Государство и право России в современном мире. Сборник докладов XII Московской юридической недели. XXII Международная научно-практическая конференция; XXIII Международная научно-практическая конференция Юридического факультета Московского

государственного университета имени М.В.Ломоносова. В 5 ч. Москва, 2023. С. 286–290.

2. Бендер Э. М. Об опасностях стохастических попугаев: могут ли языковые модели быть слишком большими? // В материалах конференции ACM 2021 года по справедливости, подотчетности и прозрачности. С. 610–623.

3. Зорькин В. Право России: альтернативы и риски в условиях глобального кризиса // Российская газета. 2022. 29 июня. URL: https://rg.ru/2022/06/29/pravo-rossii-alternativy-i-riski-v-usloviiah-globalnogo-krizisa.html (дата обращения: 05.05.2023).

4. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях // URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

5. Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО МИД России, 2021. С. 6.

6. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: Моногр. / Под общ. ред. Т.А. Поляковой. Саратов: Амирит, 2020. С. 36.

7. Обращение к читателям Министра иностранных дел Российской Федерации С.В. Лаврова // Международная информационная безопасность: теория и практика: В 3 т.: Учеб. / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект Пресс, 2021. Т. 1. С. 13.

8. Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. 2022. № 3. С. 7–15.

9. Полякова Т.А., Шинкарецкая Г.Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации

права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10. С. 138.

10. Принципы работы с ИИ, разработанные на Асиломарской конференции // URL: https://futureoflife.org/open-letter/ai-principles-russian/ (дата обращения: 24.06.2023).

11. Приоритетные направления и первоочередные задачи дальнейшего развития союзного государства на 2018-2022 годы: утверждены постановлением Высшего Государственного Совета Союзного государства от 19 июня 2018 года // URL: https://www.prlib.ru/item/1880689

12. Указ Президента РФ от 12 апреля 2021 г. № 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности" [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_381999/

13. Цифровая трансформация: вызовы праву и векторы научных исследований: Моногр. / Под общ. ред. А.Н. Савенкова; Отв. ред. Т.А. Полякова, А.В. Минбалеев. М.: РГ-Пресс, 2021. С. 62; Холодная Е.В. О правовом режиме технологии искусственного интеллекта // В книге: Права и обязанности гражданина и публичной власти: поиск баланса интересов. XVII Международная научно-практическая конференция (Кутафинские чтения) Московского государственного юридического университета имени О. Е. Кутафина (МГЮА) и XX Международная научно-практическая конференция юридического факультета Московского государственного университета имени М.В. Ломоносова (МГУ), в 5 ч.. Москва, 2020. С. 426–429.

14. Pause Giant Al Experiments: An Open Letter // URL: https://futureoflife.org/open-letter/pause-giant-ai-experiments/ (дата обращения: 24.06.2023).

Наталья Валерьевна Савельева
Международно-правовой институт МГЮА им. Кутафина,
E-mail: nasa2000@yandex.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ СПУТНИКОВОЙ СВЯЗИ ДЛЯ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА РОССИИ

Аннотация. *Статья посвящена проблеме использования Starlink в России, включает обзор международно-правового режима использования околоземного космического пространства, национального российского законодательства в части использования спутникового интернета иностранных провайдеров, анализ угроз и обоснование ограничения использования Starlink в России.*

Ключевые слова: *Старлинк, спутниковый интернет, системы спутниковой связи, технологический суверенитет, национальная безопасность.*

Введение. Компания SpaceX заявила о запуске международного роуминга Starlink, который позволяет использовать спутниковый интернет из любой точки мира. Качественным отличием группировки Starlink является недостижимое ранее число спутников, которое в настоящее время превышает 3 500, а со временем может быть увеличено до 30-40 тысяч.

Многослойность орбитальной группировки, глобальное покрытие, постоянное пополнение системы и стремительный рост числа спутников, способность спутников маневрировать и перемещаться между слоями, возможности оптической высокоскоростной связи между спутниками в дополнение к уже опробованной технологии радиосвязи с наземными станциями с минимальной временной задержкой и высокой степенью защиты канала открывают широкие возможности использования Starlink для военных целей.

В ст. 15 Стратегии национальной безопасности Российской Федерации [9] указано, что космическое пространство является новым «полигоном» для размещения оружия. Ниже дается обзор правового режима использования Starlink в космическом пространстве, приводятся примеры военного использования Starlink, а также описываются особенности законодательства и меры защиты национальных интересов России в области спутниковой связи.

Международно-правовой режим использования околоземного космического пространства, где развернут спутниковый сегмент Starlink.Согласно ст. I Договора по космосу 1967 года [1], космическое пространство открыто для использования всеми государствами на основе равенства, в соответствии с международным правом.

В п. 1 разд. А Принципов использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания 1982 года [6] указано, что при осуществлении такого вещания необходимо обеспечить паритет принципов суверенитета государства и свободного доступа граждан к информации.

В ст. IV Конвенции о передаче и использовании данных дистанционного зондирования Земли из космоса 1978 года [2], ратифицированной СССР и странами соцлагеря, закреплен запрет передачи данных дистанционного зондирования Земли (ДЗЗ) с разрешением менее 50 м без согласия зондируемого государства.

В ст. IV Принципов дистанционного зондирования Земли 1986 года [7] говорится, что деятельность по ДЗЗ должна осуществляться на основе уважения принципа полного и постоянного суверенитета всех государств и народов над своими богатствами и природными ресурсами. Согласно принципу, изложенному в ст. XII, доступ государства к информации дистанционного зондирования своей территории должен предоставляться на недискриминационной основе и на разумных условиях оплаты. В ст. XIII содержится рекомендация о проведении консультации с зондируемым государством с целью предоставления возможности участия последнего в

использовании результатов ДЗЗ, без необходимости предварительного согласия на сбор данных.

Постепенно путем «молчаливого согласия» сформировался международно-правовой обычай, что предварительного согласия зондируемого государства не требуется, а полученные данные ДЗЗ можно использовать в том числе в коммерческих целях.

В области электросвязи регулирование носит более строгий характер. Право государства блокировать распространение информации по каналам спутниковой связи закреплено в ст. 2 Конвенции о распространении несущих программных сигналов, передаваемых через спутники 1974 года [3].Согласно ст. 34 Устава Международного союза электросвязи (МСЭ) [10], государство вправе прервать любую частную электросвязь, которая могла бы представлять угрозу безопасности государства или противоречить его законам, общественному порядку или правилам приличия. В подразд. С разд. 2 ст. 9 Регламента радиосвязи МСЭ [8] указано, что государство имеет право несогласия на выделение частот при наличии помех.

Регулирование радиочастотного спектра осуществляется на трех уровнях:

1. на международном уровне — Международным союзом электросвязи МСЭ, в который входят 193 государства-члена,
2. на региональном уровне — региональными организациями, к примеру, в европейском регионе — Европейской конференцией почтовых и телекоммуникационных ведомств (CEPT), в которую входят 48 государств, в том числе Россия,
3. на национальном уровне — профильными ведомствами, в частности, в России данные функции выполняет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России), на базе которого функционирует Государственная комиссия по радиочастотам (ГКРЧ).

Чем опасен Starlink окружающей среде и интересам суверенных государств? Низкоорбитальные спутниковые системы типа Starlink создают

ряд серьезных проблем [4]. Во-первых, тысячи спутников создают серьезное световое загрязнение в оптическом и радиодиапазоне, мешают астрономическим наблюдениям. Во-вторых, в разы увеличивается объем космического мусора на низких орбитах и вероятность столкновений. В-третьих, серьезные опасения вызывает использование Starlink для военных целей.

Двойное назначение Starlink. 20 декабря 2018 года Отдел планирования стратегического развития и экспериментов ВВС США заключил со SpaceX контракт на проведение испытаний использования спутниковой сети Starlink для обеспечения военной связи [15].

В 2019 году специальные терминалы Starlink были успешно протестированы на транспортном военном самолете C-12J Huron, в рамках программы Defense Experimentation Using the Commercial Space Internet [16]. По итогам было решено использовать такие терминалы на других воздушных судах, таких как AC-130 Spectre, KC-135 Stratotanker, F-22 Raptor и F-35 Lightning II, а также на новом шаттле X-37B Orbital Test Vehicle.

В 2020 году в Радионавигационной лаборатории Техасского университета на средства ВВС США проведено исследование возможности использования спутников Starlink в качестве обработчиков и ретрансляторов сигналов GPS, чтобы многократно повысить точность позиционирования [17].

В мае 2020 года ВВС США подписали со SpaceX соглашение по использованию терминалов Starlink для обмена данными между наземными подразделениями.

В октябре 2020 года Агентство космического развития (Space Development Agency) в составе Министерства обороны США заключило со SpaceX контракт на выполнение ряда работ в рамках нового проекта по созданию национальной космической оборонной архитектуры (National Defense Space Architecture) [14], создаваемой для управления боевыми подразделениями, слежения за пусками ракет, наведения оружия.

Начиная с февраля 2022 года SpaceX было поставлено от 15 до 40 тыс. терминалов Starlink для нужд ВС Украины. Терминалы используются по сей день для обеспечения связи между тактическими подразделениями, при наведении оружия, управления БПЛА и корректировки огня артиллерии.

В августе 2022 года командованием ВВС США в Европе и Африке подписан пилотный контракт со SpaceX на предоставление услуг связи Starlink для 86-го авиакрыла ВВС США на авиабазе Рамштайн в Германии [18] с перспективой заключения масштабного соглашения с ВВС США.

В декабре 2022 года SpaceX заявила о запуске военной программы Starshield [19], в рамках которой предполагается размещение на спутниках Starlink дополнительных систем военного назначения для ДЗЗ, защищенной радио- и оптической связи для скрытой высокоскоростного обмена и ретрансляции данных с военных спутников через сеть Starlink.

Помимо связи, ведутся исследования использования Starlink для атак на космические объекты. В статье [13] показана возможность использования группировки Starlink в качестве распределённой системы орбитального перехвата, путем вывода одного или нескольких спутников Starlink на орбиты, ведущие к соударению с «недружественными» объектами. Низкая орбита, многоуровневое построение группировки, а также огромное количество спутников, связанных между собой и центрами управления на Земле бесчисленными каналами связи, позволяют превратить Starlink в потенциально-опасный инструмент, своеобразный «рой», способный провоцировать столкновения с космическими объектами.

Помимо сказанного выше, Starlink может использоваться как прикрытие при разворачивании систем дистанционного управления информационными и ударными комплексами военного назначения ВВС США: мега-группировка якобы гражданских спутников Starlink выполняет роль щита и маскировочной сети для сокрытия военных аппаратов.

Государственное регулирование спутниковой связи в России. В ч. 1 ст. 24 Федерального закона РФ «О связи» от 07.07.2003 № 126-ФЗ [12] указано,

что «использование радиочастотного спектра без соответствующего разрешения не допускается, если иное не предусмотрено настоящим Федеральным законом».

На территории России действуют правила использования спутниковых сетей связи, находящихся под юрисдикцией иностранных государств [5], согласно которым весь трафик, который исходит от спутниковых устройств абонентов из России, должен проходить через наземную станцию российского оператора связи, расположенную на территории России.

Помимо этого, операторы иностранных систем спутниковой связи должны сформировать российский сегмент в составе своей системы, а весь трафик от российских пользователей пропускать через наземные станции сопряжения в России, а также получить разрешение ГКРЧ на использование заданного частотного диапазона на территории России.

Указанные выше условия в случае Starlink не выполняются, ввиду отсутствия российского сегмента в составе наземной группировки Starlink, а также отсутствия разрешения ГКРЧ на использование частот на территории России.

Федеральным законом от 06.03.2022 № 42-ФЗ внесены изменения КоАП РФ [11], в том числе введена административная ответственность за нарушение правил использования на территории Российской Федерации спутниковых сетей связи, находящихся под юрисдикцией иностранных государств (статья 13.47 КоАП РФ).

Заключение. Защита национальных интересов нашей страны требует пристального внимание к космосу. На примере Starlink показано, что в настоящее время ведется активное освоение околоземного космического пространства для военных целей, под прикрытием коммерческих, гражданских проектов. Ограничение использования услуг иностранных провайдеров типа Starlink на территории России является оправданным, но этого недостаточно. Для укрепления технологического суверенитета России необходимо присутствие наших космический аппаратов в пространстве

вокруг Земли, развития отечественных систем спутниковой связи, таких как «Гонец», «Скиф», «Марафон».

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 // [Электронный ресурс] – URL: https://www.un.org/ru/documents/decl_conv/conventions/outer_space_governing.shtml (дата обращения: 16.05.2023)

2. Конвенция о передаче и использовании данных дистанционного зондирования Земли из космоса. Подписана в Москве 19 мая 1978 года // [Электронный ресурс] – URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/51063/ (дата обращения: 16.05.2023)

3. Конвенция о распространении несущих программы сигналов, передаваемых через спутники от 21 мая 1974 г. Подписана в Брюсселе 21 мая 1974 года // [Электронный ресурс] – URL: https://rospatent.gov.ru/ru/docs/interdocs/brussel_conv (дата обращения: 16.05.2023)

4. Пехтерев С. В., Макаренко С. И., Ковальский А. А. Описательная модель системы спутниковой связи Starlink // Системы управления, связи и безопасности. 2022. № 4. С. 190-255. DOI: 10.24412/2410-9916-2022-4-190-255

5. Правила использования на территории РФ спутниковых сетей связи, находящихся под юрисдикцией иностранных государств утв. постановлением Правительства Российской Федерации от 14 ноября 2014 г. № 1194 ФЗ // [Электронный ресурс] – URL: https://www.consultant.ru/document/cons_doc_LAW_171082/08a4e1a6f73020b7cc42b5514311f54fd06d3f06/ (дата обращения: 16.05.2023)

6. Принципы использования государствами искусственных спутников Земли для международного непосредственного телевизионного вещания. Приняты резолюцией 37/92 Генеральной Ассамблеи от 10 декабря 1982 года // [Электронный ресурс] – URL: https://www.un.org/ru/documents/decl_conv/conventions/artificial_earth_satellites.shtml (дата обращения: 16.05.2023)

7. Принципы, касающиеся дистанционного зондирования Земли из космического пространства. Приняты резолюцией 41/65 Генеральной Ассамблеи от 3 декабря 1986 года // [Электронный ресурс] – URL: https://www.un.org/ru/documents/decl_conv/conventions/earth_remote_sensing.shtml (дата обращения: 16.05.2023)

8. Регламент радиосвязи, принятый по итогам всемирных конференций радиосвязи Международного союза электросвязи в г. Женеве в 2012 и 2015 годах (вступил в силу для Российской Федерации 1 января 2017 года) // [Электронный ресурс] – URL: http://publication.pravo.gov.ru/Document/View/0001202201270013 (дата обращения: 16.05.2023)

9. Стратегия национальной безопасности Российской Федерации утв. Указом Президента РФ от 2 июля 2021 г. №400 // [Электронный ресурс] – URL: http://publication.pravo.gov.ru/Document/View/0001202107030001 (дата обращения: 16.05.2023)

10. Устав Международного союза электросвязи. Совершено в Женеве, 22 декабря 1992 г. // [Электронный ресурс] – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=201132711&collection=1&backlink=1 (дата обращения: 16.05.2023)

11. Федеральный закон «О внесении изменений в КоАП РФ» от 06.03.2022 № 42-ФЗ [Электронный ресурс] - URL: http://publication.pravo.gov.ru/Document/View/0001202203060009?index=0&rangeSize=1 (дата обращения: 16.05.2023)

12. Федеральный закон РФ «О связи» от 07.07.2003 № 126-ФЗ // [Электронный ресурс] – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102082548 (дата обращения: 16.05.2023)

13. Цыгикало Н. А. Группировка Starlink - система орбитального перехвата принципиально нового типа // Naked Science [Электронный ресурс], 28.01.2022. – URL: https://naked-science.ru/article/tech/starlink-perehvat (дата обращения: 25.09.2022)

14. Agency Awards Contracts for Tracking Layer of National Defense Space Architecture // U.S. Department of Defense official site [Электронный ресурс], 05.10.2020 - URL: https://www.defense.gov/News/News-Stories/Article/Article/2372647/agency-awards-contracts-for-tracking-layer-of-national-defense-space-architectu/ (дата обращения: 16.05.2023)

15. Contracts For Dec. 19, 2018 at U.S. Department of Defense official site [Электронный ресурс], 19.12.2018 - URL: https://www.defense.gov/News/Contracts/Contract/Article/1718270/ (дата обращения: 16.05.2023)

16. Defense Experimentation Using the Commercial Space Internet t GOVTRIBE official site [Электронный ресурс], 03.08.2017 - URL: https://govtribe.com/opportunity/federal-contract-opportunity/defense-experimentation-using-the-commercial-space-internet-fa865017s9300 (дата обращения: 16.05.2023)

17. Iannucci P. A., and Humphreys T. E., "Economical Fused LEO GNSS," 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 2020, pp. 426-443, doi: 10.1109/PLANS46316.2020.9110140.

18. Multiple Air Force Units Buy SpaceX’s Starlink Satellite Internet Service // Air & Space Forces Magazine [Электронный ресурс], 09.08.2022 - URL: https://www.airandspaceforces.com/multiple-air-force-units-buy-spacexs-starlink-satellite-internet-services/ (дата обращения: 16.05.2023)

19. Starshield. Supporting national security // SpaceX [Электронный ресурс], 10.12.2022. – URL: https://www.spacex.com/starshield (дата доступа 16.05.2023).

20. What the New SpaceX Defense Contract Means for the Starlink Project at EDGY [Электронный ресурс], 22.01.2019 - URL: https://edgy.app/spacex-defense-contract (дата обращения: 16.05.2023)

Трофимова Ольга Сергеевна
Национальный центр управления обороной Российской Федерации
Старший переводчик
E-mail: trofi.fff@gmail.com

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТРАТЕГИЙ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ И СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ

Аннотация. *2 июля 2021 года была утверждена Стратегия национальной безопасности Российской Федерации [3]. 12 октября 2022 года была утверждена Стратегия национальной безопасности Соединенных Штатов Америки [5], которая пришла на смену аналогичному документу 2017 года [4]. В статье проводится сравнительный анализ документов двух государств как основных акторов международной политики, задающих тенденции мирового развития. В работе также были использованы контент-анализ, комплексный и ценностно-нормативный методы исследования, которое опиралось, в первую очередь, на семантический разбор.*

Ключевые слова: *Стратегия национальной безопасности, соперник, угроза, противник, недружественные страны, безопасность.*

Соединенные Штаты, не скрывая своего превосходства, позиционировали себя доминирующей нацией в Стратегии национальной безопасности (СНБ) 2017 года: «Эта Стратегия национальной безопасности ставит Америку на первое место» («This National Security Strategy puts America first») [1]. Новая СНБ уже не пронизана такими яркими формулировками, но тем не менее заявляет о своих позициях весьма претенциозно. Российская Федерация при определении своего положения на международной арене обходит категоричные формулировки, которые бы заявляли об ее исключительности.

Особое внимание привлекает недвусмысленное определение Д. Трампом государств-соперников («adversaries») в 2017 году [4]: Россия,

Китай, Иран, Северная Корея. Так, по мнению бывшего президента США, Северная Корея искала возможности убить миллионы американцев с помощью ядерного оружия; Россия стремилась возродить статус сверхдержавы и установить сферы влияния вокруг границ США; «диктаторский режим» руководителей Исламской Республики Иран был направлен на дестабилизацию регионов, угрожал Америке и ее союзникам, а также приводил к жестокому обращению со своим населением; Китай развивал существующие образцы военной техники и наращивал боевую мощь, которые могли угрожать объектам критической инфраструктуры и архитектуре управления и командования США.

Изданная 12 октября 2022 года Стратегия США претерпела некоторые изменения [5]. Применительно к КНР, России, КНДР и ИРИ не используется термин «соперник» («adversary»). Китай, например – «конкурент» («competitor»), Россия тоже соперник, но с негативной коннотацией, где обе стороны обязательно ведут гонку и ненавидят друг друга («rival»), а также «угроза» («threat») («Россия представляет незамедлительную и постоянную угрозу международному миру и безопасности»). Китаю и России посвящены отдельные параграфы документа. Китай отражен и как сторона, желающая переформатировать существующий мировой порядок, и как главный торговый партнер США, с которым нужно сосуществовать. Белый дом обвиняет КНР в нанесении вреда союзникам США в Индо-Тихоокеанском регионе и по всему миру. США говорят не только за себя, но и за других: «в Европе, Азии, на Ближнем Востоке, в Африке, Латинской Америке страны четко видят, какие вызовы представляет Китай».

Очевидно, что юрисдикция США не должна распространяться на другие страны, они не могут и не должны быть вершителями правопорядка за пределами североамериканского континента в разрезе: гипотеза, диспозиция, санкция (иными словами, «если – то – иначе»).

Если обратиться к Стратегии национальной безопасности Российской Федерации 2021 г., можно увидеть в отношении других стран, не разделяющих

российские внутренний и внешний курсы, такие формулировки, как: деструктивные силы за рубежом (п. 44), недружественные страны (п. 20); ряд государств называет Россию угрозой и даже военным противником (п. 17), действия некоторых стран направлены на инспирирование в СНГ дезинтеграционных процессов (п. 17), недружественные действия иностранных государств (п. 99) [3]. Таким образом, Россия прямо не указывает государства, которые способны нанести опережающий или превентивный удар, а также выступающие угрозой безопасности РФ.

Стоит отметить, что Российская Федерация проводит последовательную и предсказуемую внешнюю политику и стремится к повышению предсказуемости в отношениях между государствами, укреплению доверия и безопасности в международной сфере. Тех же взглядов придерживается и профессор кафедры российской политики Санкт-Петербургского государственного университета Иван Владимирович Радиков, определяя в своей статье обоснованность оценки текущего состояния национальной безопасности Российской Федерации [2].

Именно Россия выступает за открытость военного планирования. Все эти положения прописаны в российской Стратегии. Как пример – открытый характер проведения операции в Сирии, к которой привлекались Воздушно-космические силы Вооруженных Сил. Только в СНБ России мы видим закрепленный принцип равной и неделимой безопасности.

Позиция Российской Федерации более взвешенная и продуманная, призывающая к сближению и общей ответственности за будущее мира, что позволит всем государствам получить больше возможностей для совместного решения глобальных проблем, выравнивания социально-экономического развития стран и регионов планеты, сбережения морального и физического здоровья человека. Россия выступает за углубление многостороннего взаимодействия без разделительных линий и блоковых подходов в целях совместного решения глобальных и региональных проблем при центральной

координирующей роли Организации Объединенных Наций и Совета Безопасности.

Заключение. Можно констатировать, что СНБ РФ носит оборонительный характер, а СНБ США редакций 2017 и 2022 годов – характер наступательный, активно отстаивающий идею экспансионизма: «Международный валютный фонд и Международный банк работают в интересах США» [5], «Америка должна стать центром притяжения всех научных ресурсов и талантливой молодежи» [5], «необходимость в сильной и целеустремленной роли Америки в мире еще никогда не была настолько значимой» [5].

Список источников и литературы:

1. Внешняя политика Трампа: «Америка на первом месте»// [Электронный ресурс] – URL: http://www.golos-ameriki.ru/amp/trump-foreign-policy/3733618.html (дата обращения: 10.05.2023)

2. Радиков И.В. Стратегия национальной безопасности России — 2021: преемственность и развитие // Политическая экспертиза: ПОЛИТЭКС. 2021. Т. 17. № 4. С. 371–386// [Электронный ресурс] – URL:https://doi.org/10.21638/spbu23.2021.404 (дата обращения: 10.05.2023)

3. Стратегия национальной безопасности Российской Федерации утв. Указом Президента РФ от 2 июля 2021 г. №400 // [Электронный ресурс] – URL: http:// www.kremlin.ru/acts/bank/47046 (дата обращения: 10.05.2023)

4. National Security Strategy. – Washington D.C.: The White House, December 2017 // [Электронный ресурс] – URL:https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 10.05.2023)

5. National Security Strategy. – Washington D.C.: The White House, October 2022 // [Электронный ресурс] – URL:https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения: 10.05.2023)

СЕКЦИЯ 5

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Воеводина Ирина Алексеевна
студент КПА РАНХиГС
E-mail: irinavoevodina03@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аннотация. *Настоящая статья посвящена вопросам использования систем искусственного интеллекта (ИИ) в области информационной безопасности. Актуальность темы обусловлена реалиями современной жизни: развитие технологий, в частности ИИ, все чаще затрагивает вопрос информационной безопасности пользователей. В статье рассматриваются преимущества и проблемы, возникающие при внедрении технологий ИИ.*

Ключевые слова: *искусственный интеллект, информационная безопасность, информационные системы и технологии, угрозы информационной безопасности, биометрия, защита информации.*

В современном цифровом мире развивается глобальное информационное общество, возрастает роль знаний, меняется система общественных отношений. Развитие информационных систем и технологий является приоритетной задачей в современном мире и с каждым годом скорость совершенствования и изменения информационного пространства лишь набирает темпы. Происходит развитие не только объема данных, количества устройств или приложений, но и самих технологий. Современный человек живет не только в мире реальном, но и в мире виртуальном. Люди все чаще доверяют компьютерам важную персональную, финансовую, социальную и медицинскую информацию. В связи с этим, информационная безопасность, с учетом внедряемых и используемых компьютерных систем, занимает важное место в современном мире. Информационная безопасность требует соблюдения конфиденциальности, целостности и доступности информации, предотвращения несанкционированного раскрытия, использования, фальсификации и уничтожения информации [2]. Внедрение информационных

сетей во все сферы человеческой деятельности привело к тому, что без использования информационных технологий, обеспечение информационной безопасности становится невозможным. В качестве такой технологии может выступать ИИ. ИИ стал активно использоваться в сфере зашиты информации, где человеку сложно найти какие-либо закономерности и решить задачу классическим алгоритмом. Возникла необходимость интеллектуальных методов оценки и постоянного мониторинга за системами. Поэтому вопросы правильного использования и улучшения защиты за счет развития информационной безопасности стали актуальным направлением в отрасли.

ИИ — это аналитическая система, обрабатывающая заданный массив исходных данных и позволяющая реализовать регламентированные, запрограммированные операции в стандартных ситуациях, а также предоставить результаты анализа оператору для принятия им решений, если ситуация не является стандартной. Использование инструментов, основанных на ИИ, обусловлено необходимостью оперативного реагирования при наступлении ситуации уязвимости системы защиты информационной безопасности. Сегодня ИИ встречается практически везде: голосовые помощники, переводчики текстов с различных языков, камеры смартфонов, умная галерея, рекомендации фильмов, возможные друзья в социальных сетях и многое другое.

Инструменты на базе ИИ отвечают различным потребностям информационной безопасности:

1. Биометрическая аутентификация. В большинстве случаев вход в аккаунт пользователя осуществляется через логин и пароль, что является самым популярным методом защиты информации, но не самым надежным и не является преградой для злоумышленников. Поэтому прибегают к биометрической аутентификации на основе ИИ. Данный метод значительно безопаснее, поскольку используются уникальные данные человека: отпечаток пальца, геометрия руки, лица, голос и т.д. [3].

2. Быстрое реагирование на атаки. Простое выявление угроз в режиме реального времени не имеет смысла, если система не способна бороться с угрозами и предотвращать их, прежде чем они нанесут ущерб. Когда происходит атака системы, ИИ автоматически предлагает планы по предотвращению атаки [1].

3. Перспективным на сегодняшний день также является такое направление ИИ, как «поведенческая биометрия». ИИ не просто умеет распознавать голос, отпечаток пальца или лицо пользователя, а анализирует специфику его активности: клавиатурный почерк, особенности движений при работе с мышью, сенсорной панелью. Важным преимуществом поведенческой биометрии является то, что отслеживание аутентичности предусмотрено в непрерывном режиме, в процессе работы пользователя с устройством.

При этом нельзя сказать, что современные методики защиты данных посредством ИИ совершенны. Угрозы информационной безопасности возросли с распространением Интернета, вместе с тем ИИ прибавляет новые точки возможных атак. Необходимо отметить, что на этапе подготовки хакерских атак уже сейчас многие злоумышленники используют ИИ и таким образом планирование и осуществление атак становится более продуманным и приобретает большие шансы на успех. Известны мошеннические приемы использования реалистичного виртуального образа человека (Deepfake) для обмана систем, подделки голосов для мошеннических звонков, применения телефонных технологий для фишинга и хищения денежных средств. Также используются элементы ИИ, которые позволяют атакующим быстрее повышать свои привилегии, перемещаться по корпоративной сети, а затем находить и похищать интересующие их данные. Технологию ИИ используют для несанкционированного доступа к различным базам и аккаунтам пользователей, а также для создания вредоносного программного обеспечения. Для того, чтобы ИИ смог обеспечить требуемый уровень защиты информации, он должен быть корректно реализован, интегрирован в существующие системы и обучен [4].

Заключение. Таким образом, информационное право должно ответить на вызовы современного мира и технологий, включая задачи развития искусственного интеллекта и формирования системы противодействия информационной преступности. Мы живем в эпоху, когда центральной проблемой для пользователей стала информационная безопасность, так как масштабы преступности постоянно растут. Большинство современных решений в сфере информационной безопасности так или иначе основаны на ИИ. При этом внедрение ИИ в область защиты информации сопряжено с массой рисков. В связи с этим, важно понимать, что развитие новых технологий, таких как ИИ, может нанести колоссальный ущерб большинству сфер деятельности людей, поэтому необходимо регулировать развитие данной сферы на законодательном уровне. Меры по противодействию различным информационным атакам должны быть приняты уже сегодня, поэтому изучение атак, основанных на ИИ, и поиск способов противодействия им является важнейшим вопросом современности.

Список источников и литературы:

1. Афанасьева Д.В. Применение искусственного интеллекта в обеспечении безопасности данных // Известия Тульского государственного университета. Технические науки. — 2020.

2. Куренная В.О. Искусственный интеллект в информационной безопасности // Научно-образовательный журнал «StudNet». — 2022.

3. Окатов Д.А., Минеева Т.А. Технологии искусственного интеллекта в информационной безопасности // Журнал «Тенденции развития науки и образования». — 2021.

4. Шананин В.А. Применение систем искусственного интеллекта в защите информации // Журнал «Инновации и инвестиции». — 2022.

Жеребятьев Данил Евгеньевич
студент кафедры кибербезопасности и защиты информации, ФГБОУ ВО
«Кубанский государственный технологический университет»,
E-mail: zdanil.ty@gmail.com

Калюжный Денис Станиславович
студент кафедры кибербезопасности и защиты информации, ФГБОУ ВО
«Кубанский государственный технологический университет»,
E-mail: kalyuzhnyds@gmail.com

АСПЕКТЫ ПРИМЕНЕНИЯ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Аннотация. *Данная статья посвящена исследованию возможностей применения алгоритмов машинного обучения для обнаружения и предотвращения несанкционированного доступа со стороны злоумышленников. В ней рассмотрены основные методы обнаружения уязвимости компьютерных систем, а также применение машинного обучения для обнаружения и предотвращения кибератак. Также в статье рассмотрены преимущества и риски применения машинного обучения в кибербезопасности. В заключении подчеркивается необходимость дальнейших исследований в этой области.*

Ключевые *слова: информационная безопасность, машинное обучение, несанкционированный доступ, кибербезопасность, защита информации.*

Киберпреступность стала одной из самых серьезных угроз безопасности современного цифрового мира. Несанкционированный доступ со стороны злоумышленников приносит огромный ущерб, как отдельным компаниям, так и всему сообществу в целом. Ежегодно публикуется статистика киберпреступлений, которые охватывают все сферы жизни и деятельности общества, включая организации критически важной инфраструктуры для государства [3]. Каждый день злоумышленники используют все новые и новые методы для взлома защиты, что требует от индустрии информационных технологий постоянного усовершенствования методов защиты [1]. Вместе с

этим, развитие технологий совершенствует и возможности применения искусственного интеллекта, расширяя инструментарий обеспечения информационной безопасности [7].

В этой связи необходимо постоянно искать новые методы защиты информации и совершенствовать механизмы предотвращения кибератак, где машинное обучение может стать инструментом решения в ответ на вызовы, связанные с технологическим развитием общества.

Современные методы обнаружения уязвимости компьютерных систем включают в себя: статический анализ кода, динамический анализ поведения системы, анализ сетевого трафика, а также использование систем обнаружения вторжений.

Статический анализ кода – метод обнаружения несанкционированного воздействия на вычислительную систему специальными программными средствами, который основан на анализе программного кода на предмет наличия уязвимостей и потенциальных угроз без запуска приложения. Этот метод может использоваться для обнаружения уязвимостей в исходном коде приложений и операционных систем, а также дает возможности выявить уязвимости, такие как SQL, переполнение буфера, неправильную обработку ввода пользователей и другие типы атак, которые могут быть использованы для взлома системы. Динамический анализ поведения системы основан на мониторинге поведения системы в режиме реального времени, что позволяет обнаружить атаки, которые используют новые методы и неизвестные уязвимости. Динамический анализ может использоваться для обнаружения атак, таких как вредоносные программы, ботнеты, DDoS-атаки и другие типы кибератак [2].

Анализ сетевого трафика – метод обнаружения кибератак, который основан на анализе трафика в сети и используется в целях выявления сетевых аномалий, которые могут быть связаны с несанкционированным доступом. Этот метод может использоваться для обнаружения атак, таких как

сканирование портов, перехват трафика, внедрение вредоносных программ и других типов атак.

Использование системы обнаружения вторжений – метод обнаружения кибератак, который основан на использовании специальных систем для мониторинга и обнаружения угроз. Эти системы могут использоваться для обнаружения атак, таких как DDoS-атаки, взломы паролей, внедрение вредоносных программ и других типов атак. Они позволяют быстро обнаруживать угрозы и принимать меры для их предотвращения.

В настоящее время рассматривается перспектива применения машинного обучения для обнаружения несанкционированное воздействия на информационно-компьютерные технологии по всем направлениям информационной защиты, включая анализ журналов систем [9].

Так, предполагается, что многие вредоносные программы могут быть определены на основе своих характеристик, таких как их сигнатуры, поведение и т.д. В этой связи перспектива применения машинного обучения состоит в разработке модели, которая будет классифицировать вредоносные программы на основе их характеристик. Типовым использованием машинного обучения должно стать обнаружение аномалий в сетевом трафике, где модель может быть обучена на основе нормального поведения сети и использоваться для обнаружения аномальных пакетов данных.

Машинное обучение может быть использовано для обнаружения аномального поведения пользователей, которое может указывать на попытки кибератак. Модель может быть обучена на основе типичного поведения пользователей и использоваться для обнаружения аномальных действий [8]. Однако необходимо учитывать, что модели могут иметь ложноположительные и ложноотрицательные результаты, и требуется тщательный анализ результатов для снижения риска ошибок.

Существует ряд неоценимых преимуществ применения методов машинного обучения в кибербезопасности, среди которых следует отметить скорость обработки данных, возможность выявления угроз до наступления

инцидентов [4]. Вместе с этим, немаловажным фактором является точность, т.к. ручной анализ данных приводит к погрешностям и ошибкам. Следовательно, машинное обучение значительно повышает точность и уменьшает вероятность ошибок, позволяет автоматизировать процессы и уменьшить нагрузку на персонал. Машинное обучение позволяет постоянно мониторить системы без остановки, что уменьшает риски.

Однако применение машинного обучения в обеспечение информационной безопасности организаций также имеет свои недостатки:

– Несовершенство алгоритмов и долгосрочность процесса обучения. Машинное обучение может допускать ошибки, если алгоритмы не настроены должным образом [6]. В свою очередь, правильная настройка алгоритмов – долгосрочный процесс, где временной фактор также можно отнести к недостаткам применения инструментов машинного обучения в кибербезопасности.

– Недостаток данных и актуальность статистической базы. Машинное обучение требует большого количества данных для обучения, и если эти данные недоступны, то результаты могут быть недостаточно точными. В России процесс сбора данных организован сложнее, чем в зарубежных странах в связи с особенностями статистического учета.

– Случайные результаты. Машинное обучение может дать непредсказуемые результаты, которые не всегда правильно отражают суть поставленной задачи, что может привести к неправильным решениям и нанесению ущерба [10]. Здесь следует отметить, что попытки переобучения алгоритмов не всегда имеют положительный результат.

– Зависимость от технологического обновления. При отсутствии механизма совершенствования алгоритмов машинного обучения, применяемые методы устаревают. В этой связи, применение машинного обучения может создать зависимость от технологии, что может привести к уязвимостям и рискам.

Машинное обучение имеет большой потенциал в обеспечении информационной безопасности организаций и может быть использовано для различных целей, таких как обнаружение взломов, предотвращение атак и анализ угроз безопасности [5]. Для достижения оптимальных результатов, необходимо решить несколько проблем, таких как сбор и обработка данных, разработка эффективных алгоритмов и моделей, а также увеличение точности и надежности системы. Актуальной задачей в использовании машинного обучения – постоянный поиск «правильных» алгоритмов и повышение масштаба выборки для обеспечения достаточного количества данных в процессе обучения. Также важно учитывать риски и принимать меры для их минимизации. Дальнейшие исследования в области машинного обучения в кибербезопасности могут помочь устранить некоторые из этих проблем и раскрыть новые возможности. Например, использование глубокого обучения может значительно улучшить точность системы обнаружения взломов, а обучение с подкреплением может улучшить системы предотвращения атак. В целом, машинное обучение имеет огромный потенциал в кибербезопасности и может быть эффективным инструментом в борьбе с несанкционированным доступом со стороны злоумышленников. Однако, для достижения лучших результатов, необходимо продолжать исследования и улучшать существующие системы.

Заключение. В заключение следует отметить, машинное обучение является только одним из инструментов в борьбе с киберугрозами и должен применяться в дополнении или в комбинировании с другими инструментами и методами защиты информационной безопасности компьютерных систем, т.к. не может заменить человеческий фактор и экспертизу. Поэтому, дальнейшие исследования также должны учитывать вопросы этики и приватности, а также обеспечение прозрачности и объяснимости принимаемых системой решений.

Список источников и литературы:

1. Берлин С. И., Козырь Н. С. Цифровизация экономики в обеспечении экономической безопасности РФ: наукометрический анализ // Естественно-гуманитарные исследования. – 2022. – № 40(2). – С. 46-52.

2. Оганесян Л. Л. Проблемы и перспективы применения новых технологий дизайна в социокультуре // Естественно-гуманитарные исследования. – 2021. – № 33(1). – С. 178-180.

3. Козырь Н. С., Бирбасова А. В. Аспекты идентификации объектов критической информационной инфраструктуры РФ // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 2. – С. 163-172.

4. Классификация механизмов атак и исследование методов защиты систем с использованием алгоритмов машинного обучения и искусственного интеллекта / И. В. Володин, М. М. Путято, А. С. Макарян, В. Ю. Евглевский // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 2(54). – С. 91-98.

5. Козырь Н. С. Методические подходы риск-менеджмента информационной безопасности // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2023. – № 4. – С. 72-79.

6. Путято М. М., Макарян А. С. Исследование возможности совершенствования кибербезопасности инфраструктуры интернета вещей на основе интеграции биометрических методов аутентификации // Информационные системы и технологии в моделировании и управлении: Сборник трудов V Международной научно-практической конференции. – Ялта: Ариал, 2020. – С. 267-270.

7. Седых Н. В., Фоканов И. П. Проблемы и перспективы развития технологии искусственного интеллекта // Естественно-гуманитарные исследования. – 2022. – № 44(6). – С. 266-267.

8. Хализев В. Н., Федоров С. Ю., Жданова Н. В. Математическая модель синтеза интегрированной системы безопасности на основе теории игр и

применения квалиметрической оценки качества // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 3(29). – С. 43-49.

9. Частикова В. А., Шелудько М. А. Реализация экспертной системы для определения актуальных угроз безопасности информации предприятий // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2022. – № 3. – С. 80-89.

10. Шарай В. А., Сорокина А. В. Алгоритмическое обеспечение системы адаптивного мониторинга компьютерных сетей // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2018. – № 3. – С. 396-408.

София Сергеевна Забелич
Отдел внешних церковных связей
Московского Патриархата,
РГГУ
факультет «Международные отношения в Евразии»
бакалавриат
E-mail: sofiya.zabelich@bk.ru

КОРРЕЛЯЦИЯ ВНЕШНЕПОЛИТИЧЕСКИХ РЕШЕНИЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

«...если бы среди философов установилось согласие относительно значения слов, то почти все их споры были бы прекращены».

«Правила для руководства ума». Р. Декарт

Аннотация. *В статье рассматриваются технологии применения искусственного интеллекта во внешнеполитических процессах. ИИ, являясь частью системы международных отношений, влияет на мировоззрение и поведение акторов этого изменчивого процесса. Рассмотрены предвыборные кампании в Южной Корее, Турции и США. Данная статья представляет видение проблем, связанных с изучением и имплементированием ИИ в обществе.*

Ключевые слова: *искусственный интеллект, дипфейк-аватар, нейронная сеть, Cambridge Analytica, политтехнологии, алгоритмы подделок, международная система безопасности, Интернет, doomscrolling, Facebook.*

Искусственный интеллект (ИИ), как отличительная черта Четвёртой промышленной революции [1], существенно влияет на ход политических процессов. Дипломатию можно назвать «игрой слов», однако сегодня конкуренцию им составляют цифры и технологии, способные генерировать миллионы слов и значений, создавая универсальные возможности для манипуляций общественным сознанием. Прошло почти половина столетия, когда в концепции «Крошка-машина» (Baby Machine) Алана Тьюринга,

сформированной на «Дармутском летнем исследовательском проекте по вопросам искусственного интеллекта» (1956 г.), было начата дискуссия о том, что «любой аспект интеллектуальной деятельности человека можно описать так, что машина будет способна его воспроизвести [2]».

Современные внешнеполитические реалии требуют быстрого принятия решений, поэтому применение ИИ особенно актуально. Однако стоит отметить, что технологии развиваются быстрее, чем их правовое урегулирование и дипломатические возможности. Вести диалог о формировании «правил игры» нужно как можно интенсивнее, чтобы остановить склонность некоторых международных акторов уклоняться от исполнения мультилатеральных обязательств.

Сфера ИИ делится на три типа: слабый, средний и сильный. На использование «среднего ИИ», имеющего элементы адаптивного самообучения и самосовершенствования по мере накопления данных и алгоритмов, сделано большинство ставок. Наиболее спорной областью является создание и использование «сверх-ИИ»[3], так как по многим показателям данный тип превосходит развитие человека. Его неравномерное встраивание в естественный ход политического процесса внутри государств при отсутствии достаточной проработки на законодательном уровне, способен коренным образом менять общую международную систему безопасности.

Сегодня в рамках дестабилизации обстановки внутри государств используются кибератаки с применением технологий ИИ с высоким уровнем социальной инженерии и применением комбинированных систем. Технологии применяются с целью управления и манипулирования народными массами, их информационной поддержки и сопровождения, возведения в ранг «народных» протестных выступлений, склонение действующих властей к принятию требований протестующих, даже если они наносят национальный ущерб интересам государства. В процессе подобных дестабилизационных ситуаций широко применяются фейки и различные элементы гибридного воздействия цифровых технологий. Широко используются возможности нейронных сетей,

таких как реккурентные (Recurrent Neural Network, RNN), сверточные нейронные сети (Convolutional Neural Network, CNN) и генеративно-состязательные сети (Generative Adversarial Network, GAN), которые являются своего рода алгоритмами, которые способны создавать новые данные из существующих наборов датасетов. Например, GAN может анализировать тысячи записей голоса конкретного человека, а затем на основе этого анализа создать полностью новый аудиофайл с таким же точно голосом, использующим те же самые речевые шаблоны.

Также высокими темпами развивается направление нейроморфной электроники, когда искусственные нейронные сети имитируют биологические нейроны. Внимания заслуживает проект «Блю Брейн» (Blue Brain Project) [4], в котором исследуется работа ансамблей нейронов, а структура «Синапс Икс»(SyNAPSE X) [5], финансируемая программой DARPA и корпорацией IBM, уже давно занимается созданием физической копии человеческого мозга, воплощённой в виде микросхем с искусственными нейронами.

Разработка и применение подобных технологий вызывает определённую тревожность. Цель дестабилизации обстановки внутри государства с применением технологий ИИ – это генерирование протестного потенциала в обществе и политической сингулярности, что в итоге способно привести к дискредитации и инфляции власти в стране.

Беспокойство также вызывает доступность дипфейков (Deep Fakes), возможность быстрого использования и распространения фейковых аудио-и видеозаписей. Deep Fake публичного лица может существенно повлиять на результаты выборов. Такой стратегией, основанной на глубокой подделке, воспользовался нынешний президент Южной Кореи Юн Сок Ёль [6]. Оппозиционный политик и кандидат от консервативной партии «Сила народа» в период предвыборной кампании успешно применил технологию глубокой подделки с помощью дипфейк-аватара AI Yoon [7], созданного на базе американского стартапа DeepBrain, специализирующегося на синтезе речи, видео и обработке языка с помощью технологий ИИ. Юн Сок Ёль записал

около 3000 предложений, 20 часов аудио- и видеозаписи, чтобы предоставить достаточное количество данных для аватара и в итоге получил цифрового двойника, с помощью которого выборная кампания стала проводиться в нескольких местах одновременно. Двойник использовал интересные выражения, опускал шутки в адрес действующих политиков в попытках понравиться молодым избирателям, голосов которых не хватало для победы реальному южнокорейскому кандидату [8]. Дипфейк-аватар также использовал язык, используемый в мире онлайн игр, что повысило популярность Юн Сок Ёля среди молодого населения.

Опыт данной президентской кампании показывает новую фазу использования технологий ИИ в политическом процессе с целью манипуляции человеческим сознанием. Возникает соответствующий вопрос: что делать, если искусственно разработанный образ государственного деятеля помог реальному человеку, без соответствующих качеств интеллекта и характера, занять высокую должность? Беспокойство также вызывает и тот факт, что законодательные меры для борьбы с подобными угрозами отсутствуют от развития инструментов искусственного интеллекта, а иногда и вовсе отсутствуют.

Привлечение технологий ИИ в выборные кампании не всегда успешно и может со временем поставить крест на многих политтехнологиях. Быстрота взаимодействия искусственного интеллекта с данными, его возможности погенерации информации могут играть на руку тем силам, которые имеют административные и специальные ресурсы для перехвата власти. Так, дипфейки и боты с применением искусственного интеллекта были использованы для влияния на электорат в течение президентских выборов в Турции [9]. Участие ИИ в выборах несколько изменило стратегию компании, привнеся в неё элементы грязного политического трюка. Порнозаписи и боты с заведомо ложной информацией были использованы против одного из кандидатов в президенты Турции Мухаррема Индже – председателя партии «Родина». Ему пришлось снять свою кандидатуру за три дня до выборов [10],

обвинив своих оппонентов в попытках уничтожить его репутацию, посредством публикации порнодипфейков и ряда денежных переводов на счета его сына.

Подобные скандалы негативно влияют на общество. Думскроллинг (doomscrolling) [11], чрезмерное погружение в новостную ленту, наполненную плохими новостями, плохо сказывается на качестве жизни и тонусе человека. Сова мудрости Минервы вылетает в полночь, т.е. осознание обывателем возможностей ИИ приходит намного позже, когда уже невозможно избежать последствий плодов сотворённого. Бездумно продвигаясь по пути технологического совершенства ради развлечения и удовлетворения, человечество может пересечь ту черту, за которую придётся заплатить неподъёмную этическую цену.

Определённо активным на сегодняшний день является развитие обработки естественного языка (NLP) и активация данных социальных сетей о своих пользователях. Примечательно воздействие «больших данных» (Big Data) на мировую политику можно наблюдать в деятельности компании Cambridge Analytica, ресурсы которой привлекались в предвыборной кампании Дональда Трампа в 2016 году [12].

Как утверждает компания, а также расследование [13] швейцарского журнала «Дас Магацин» (Das Magazin), посвящённое её деятельности во время избирательной кампании и голосования по Брексит (Brexit), специалисты с помощью различных способов воздействия на избирателей через соцсети убедили многих пользователей проголосовать именно за Д.Трампа 8 ноября. Группа политтехнологов из Cambridge Analytica воздействовала на электорат через соцсети посредством сочетания психографики с сетевым отбором персональных данных. Таким образом компания получила базу психометрических данных с возможностью адресного обращения к миллионам американцев и британцев.

База данных включала в себя психологические портреты людей на основе 5 тыс. различных параметров. Учитывались политические пристрастия

пользователей, предпочтения телевизионных программ, интернет-покупки, а также лайки, сохранённые посты, картинки, музыка и даже адреса проживания отдельных граждан. Избиратели также проходили анонимные тесты, в ходе которых определялась степень доверия к власти, законопослушность, откровенность и степень ответственности. Все данные были обработаны, и запущена таргетированная политическая агитация, обеспечивающая получение реципиентами сообщений, максимально соответствующих их социальным и политическим пристрастиям. Компания сыграла ключевую роль в успехе Трампа, располагая данными от 50 млн. до 87 млн. человек американских и британских пользователей (по оценке The New York Times [14] (NYT) и признаниям Facebook[4]), разработав которые превратила в инструменты массового убеждения.

Можно клеймить экосистему компании, которая собирает личные данные в обмен на контент, общение и развлечение. Но на самом деле это лишь отличительная внутренняя черта любой социальной сети, которая сочетает в себе психографику с сетевым сбором персональных данных, ради формирования полного представления о целевой аудитории и классификации групп населения в соответствии с психологическими переменными. А любая технология, направленная на сбор информации и не несущая в себе «сознательный» и позитивный разум (каким обладает человек), способна принести больше отрицательных последствий, чем отсутствие информации вовсе.

Вмешательство Cambridge Analytica во внешнеполитические процессы было отмечено не только в США. Расследования британской программы «Новости четвёртого канала» (Channel 4 News)[15], The Guardian [16] показали, что компания посредством сбора данных вмешивалась в политические процессы в более чем в 200 странах: в Чехии, Аргентине, на Шри-Ланке и др. Обо всём этом рассказал сам владелец компании Александр Никс, когда к нему под видом

[4] *Платформа признана экстремистской организацией. Деятельность запрещена в Российской Федерации.*

клиентов, желающих повлиять на предстоящие выборы, приходили журналисты. Никс также поведал о способах изменения человеческих лиц, которые могли применяться в ходе предвыборных кампаний и об использовании материалов, компрометирующих кандидатов.

Пример с Cambridge Analytica наталкивает на мысль о том, что сегодня уже довольно трудно найти грань, за которой начинаются манипуляции над обществом и вмешательство в процесс принятия внешнеполитических решений. Если убрать существование факта, согласно которому компания помогала Д.Трампу набрать необходимое количество голосов во время выборной гонки, то, назревает болезненный вопрос: оказание влияния на миллионы – это суть самого Facebook[5] или воля политтехнологов? Ведь в целом политика интернета и состоит в том, чтобы, используя данные о пользователях, предлагать привлекательные для них сервисы, рекламу, коммуникации и развлечения. Интернет – это сервис в обмен на воздействие. Важно также учитывать, что изначально в Facebook заложены алгоритмы, позволяющие анализировать лайки, сохранения и переходы в профили пользователей. Алгоритм фильтрации новостей (Edge Rank [17]), анализирующий наше поведение в Facebook, по сути, создаёт тот же психологический профайл, только не на 50-70 млн, как в предвыборной гонке Трампа, а на 2 млрд человек по всему земному шару.

Применение технологий ИИ в решении многих глобальных вызовов актуализирует необходимость изучения возможностей ИИ в процессе принятия внешнеполитических решений. Однако не стоит предполагать, что в будущем «государство 2.0» интегрирует в себя самые передовые технологии и превратится в безошибочную машину. Здесь нет места логике трансгуманизма [18], [19]. Необходимо проводить чёткую границу между «законодателями» и «администраторами»[20]. На современном политическом языке, народ должен определять политику, а технологии ИИ, если они применяются в управлении государством, находить оптимальные пути для

[5] *Платформа признана экстремистской организацией. Деятельность запрещена в Российской Федерации*

реализации воли людей. Именно здесь, в политике искусственный интеллект будет кибернетическим, т.е. потребуется более тщательное интегрирование человеческих процессов с машинными. В будущем «государство 2.0» может быть киборгом, но, человек должен остаться актором в политической системе. Для достижения этого своегообразного компромисса необходим законодательный механизм, система международной информационной безопасности, которая предполагает принятие всем мировым сообществом принципов сетевого равенства, равноправия и децентрализованного управления Интернетом.

Заключение. Стоит отметить, что не следует отказываться от использования ИИ в формировании и реализации внешней политики: в процессе имплементации приоритеты должны отдаваться аугментации. Таким образом, искусственный интеллект будет развиваться не как арбитр и реформатор международных отношений, а как вспомогательный инструмент, что существенным образом сократит потенциальные возможности рисков.

Список источников и литературы:

1. О пределах государственной деятельности / Вильгельм фон Гумбольдт; пер. с нем. — Челябинск: Социум, 2009. — 287.

2. Четвертая промышленная революция / К. Шваб — «Эксмо», 2016 — (Top Business Awards).

3. A Global Arms Race to Create a Superintelligent AI is Looming. URL: https://www.vice.com/en/article/xywmyk/a-global-arms-race-to-create-a-superintelligent-ai-is-looming (date of access 15.05.2023).

4. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence John McCarthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. 2006, p. 12.

5. AFP (2022) Deepfake democracy: South Korean candidate goes virtual for votes. In: France 24. URL: https://www.france24.com/en/live-news/20220214-deepfake-democracy-south-korean-candidate-goes-virtual-for-votes. (date of access: 12.05.2023).

6. AFPRelaxnews (2022) Deepfake Democracy: South Korean Presidential Race Candidate Goes Virtual For Votes. In: Forbes India. URL: https://www.forbesindia.com/article/lifes/deepfake-democracy-south-korean-presidential-race-candidate-goes-virtual-for-votes/73715/1 (date of access: 12.05.2023).

7. Becoming Machines Is Part of Our Destiny,' Says Transhumanist Zoltan Istvan [Podcast]. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.69e174f5-6477561c-f345b10a-74722d776562/https/reason.com/podcast/2017/09/07/transhumanism-libertarianism-zoltan/ (date of access: 15.05.2023).

8. Bostrom N. (2014) Superintelligence: Paths, Dangers, Strategies. Oxford: Oxford University Press. 352 p.

9. Cambridge Analytica Uncovered: Secret filming reveals election tricks – YouTube. URL: https://www.youtube.com/watch?v=mpbeOCKZFfQ (date of access: 20.04.2023).

10. Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' – YouTube. URL: https://www.youtube.com/watch?v=FXdYSQ6nu-M (date of access: 20.04.2023)

11. Deepfakes, porn tapes, bots: How AI has shaped a vital NATO ally's presidential election. URL: https://www.foxnews.com/world/deepfakes-porn-tapes-bots-ai-shaped-vital-nato-allys-presidential-election (date of access: 30.05.2023).

12. Donald Trump's mind readers try to win him voters. CNN Politics. URL: https://edition.cnn.com/2016/11/04/politics/donald-trump-political-ads-cambridge-analytica/index.html (date of access: 12.05.2023).

13. Doomscrolling: the Word for Staying up Late Reading Coronavirus News. URL: https://www.businessinsider.com/doomscrolling-explainer-coronavirus-twitter-scary-news-late-night-reading-2020-4 (date of access: 10.05.2023).

14. Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens - The New York Times. URL:

https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (date of access: 24.05.2023).

15. Fall Cambridge Analytica: Facebook erzielt Einigung im Prozess wegen Datenmissbrauchs | Tages-Anzeiger. URL: https://www.tagesanzeiger.ch/facebook-erzielt-einigung-im-prozess-wegen-datenmissbrauchs-259466349367 (date of access: 26.06.2023).

16. GitHub - BlueBrain/nexus: Blue Brain Nexus - A knowledge graph for data-driven science. URL: https://github.com/BlueBrain/nexus (date of access: 09.04.2023).

17. Muharrem İnce adaylıktan çekildi! Sosyal medyadan bir açıklama daha yaptı - Haber 7 SİYASET. URL: https://www.haber7.com/siyaset/haber/3324116-muharrem-ince-adayliktan-cekildi-sosyal-medyadan-bir-aciklama-daha-yapti (date of access: 24.05.2023).

18. Synapse X URL: https://x.synapse.to/ (date of access: 27.06.2023).

19. The deepfake avatar of a presidential candidate revolutionizes the electoral campaign in South Korea - American Chronicles. URL: https://www.americanchronicles.news/the-deepfake-avatar-of-a-presidential-candidate-revolutionizes-the-electoral-campaign-in-south-korea/ (date of access: 12.05.2023).

20. Understanding EdgeRank: How Facebook’s Algorithm Actually Works. URL: https://buffer.com/resources/understanding-facebook-news-feed-algorithm/ (date of access: 29.05.2023).

Поднебесная Юлия Борисовна
магистрант
МГУ имени М.В. Ломоносова
E-mail: ya.yulaya@yandex.ru

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИЗРАИЛЕ

Аннотация. *Израиль является одним из мировых лидеров в сфере искусственного интеллекта на 2023 год. В работе рассмотрены причины успехов Израиля в данном направлении, исследованы факторы, позволяющие ИИ успешно развиваться в Израиле на протяжении своего существования. Представлен анализ взаимодействия Израиля с международными акторами мировой политики в области ИИ, оценены перспективы сотрудничества и масштабы угроз. В выводах работы содержится прогнозы о дальнейшем развитии ИИ в Израиле.*

Ключевые слова: *Израиль, искусственный интеллект, правовой статус, международное сотрудничество, рейтинг, ТНК, армия, Ближний Восток.*

На данный момент Израиль лидирует в сфере разработок, касающихся искусственного интеллекта (ИИ). Согласно данным Национального совета по научными исследованиям и развитию при Министерстве науки Израиля, около 898 компаний вовлечены в сферу этой деятельности, что включает в себя такие направления, как большие данные (big data), машинное обучение (machine learning), интеллектуальные системы и программы и др. [5]. По данным Oxford Insights, Израиль находится на 20-м месте (из 181) по индексу готовности среди государств к применению ИИ на 2022 г [14]. Среди стран Ближнего Востока Израиль является региональным лидером в сфере ИИ, имеет показатель индекса 70.12 по 100-балльной шкале, в то время как средний показатель по миру – 44.61 [15]. Следует отметить, что Израиль лидирует и в своём регионе, и среди стран MENA [16]. Эти позиции государство сохраняет во многом благодаря тому, что его показатель по компоненту

технологического сектора намного выше, чем у других стран как в регионе MENA, так и среди остальных стран мира; Израиль занимает четвертое место по этому компоненту в целом. Рассмотрим, что привело к сложившейся ситуации.

Во-первых, многие израильские компании ещё в 90-е годы XX в. начали заниматься развитием ИИ, что сейчас принесло большие плоды. Например, израильская компания Mobileye [13], которую впоследствии приобрела компания Intel.

Во-вторых, Израиль вкладывает большие инвестиции как в кибербезопасность, так и конкретно в сферу ИИ. 16% мировых инвестиций в киберпространство приходится на Израиль. В 2020 году израильский киберэкспорт достиг 6,85 млрд долларов, а объем инвестиций — 2,9 млрд долларов [17]. Что касается вложений в ИИ, уже в 2018 году 37% привлечённых инвестиций приходились на компании, занимающиеся им [10]. По последним данным, национальная программа по продвижению ИИ в Израиле подразумевает сумму в 2 млрд. шекелей [7]. То есть новые технологии, в том числе и ИИ, в Израиле достаточно финансируются, чтобы иметь возможность успешно развиваться.

В-третьих, в Израилесуществует развитая культура стартапов. Об этом говорила ещё Голестан Радван, бывший советник министра по вопросам ИИ в Министерстве связи и информационных технологий Египта [15]. В Израиле самое большое число стартапов на душу населения - 1 стартап на 1 400 человек [3]. По рейтингу Глобального Инвестиционного Индекса на 2022 год Израиль занимает 16-ое место среди всех стран мира и первое место среди стран ближневосточного региона [4]. Также в стране существует Ведомство по инновациям (Israel Innovation Authority) [18], что тоже благоприятно сказывается на развитии ИИ, поскольку ведомство покрывает 85% расходов инновационных стартапов, позволяя ИИ развиваться во множестве сфер: от автотранспорта до медицины.

В-четвёртых, многие иностранные компании сотрудничают с Израилем в области ИИ. Израиль обладает способностью создавать важные партнерские отношения с транснациональными компаниями и выгодные проекты с учеными за пределами региона, которые помогают позиционировать страну на мировой арене ИИ. Доля Израиля в глобальной индустрии ИИ составляет 11%, страна занимает третье место в мире по данному показателю после КНР и США [12].

Но несмотря на такое повсеместное использование Израилем ИИ и огромное количество успешно функционирующих международных связей в этой области, существуют некоторые сложности в использовании и применении израильского ИИ.

Первая из них – правовой статус. Эта сложность связана с тем, что в Израиле отсутствует закон об ИИ, то есть деятельность такой быстро развивающейся отрасли не полномасштабно регулируется государством на законодательном уровне. Конечно, это не единственная страна, в которой на данный момент деятельность, связанная с ИИ, искусственного интеллекта ещё не регламентирована в правовой системе: напротив, по разным оценкам, всего чуть более тридцати стран вообще имеют стратегии развития ИИ [2]. Направление новое, далеко не все страны успели подготовить достаточную базу для юридического статуса ИИ, да и не во всех государствах он так активно развивается, чтобы на данный момент в этом действительно была необходимость. Тем не менее, этого нельзя сказать про Израиль. При таких темпах и многолетней истории развития ИИ, при постоянных инвестициях, логичным было бы наличие каких-либо государственных документов, определяющих статус ИИ и регулирующих его деятельность. Поэтому в июле 2022 года на конференции в Тель-Авиве была представлена израильская Национальная программа по искусственному интеллекту, одно из положений которой предусматривает «решение нормативных и этических вопросов в сфере использования искусственного интеллекта» [7]. Тем не менее, спустя почти год, чёткой нормативно-правовой базы так и не было представлено. Чем

обусловлено такое положение дел? Проблема в том, что всестороннее законодательное регулирование ИИ было бы не выгодно самому Израилю.

Израиль основательно намерен использовать ИИ в своей армии. Институт исследований национальной безопасности (Institute for National Security Studies, INSS) подробно рассказывает о многочисленных военных применениях ИИ как существующих, так и будущих. Одним из примеров являются автономные системы вооружений, такие как роботы и дроны, которые способны самостоятельно искать, идентифицировать и атаковать цели, практически без участия человека [11]. Израиль уже имеет значительные разработки в этой сфере и прекращать их не намерен, что подтвердил отказом присоединиться к глобальному соглашению, регулирующему использование ИИ в военной сфере [8]. И это вторая большая сложность для всего мирового сообщества, связанная с развитием ИИ в Израиле – израильский военный потенциал в области ИИ.

Такая позиция Израиля идёт вразрез с тенденцией развитых стран регламентировать использование ИИ. Многие акторы мировой политики стремится ограничить деятельность ИИ в военной сфере [19], принимают другие законы, ограничивающие использование ИИ [6]. Но Израиль на данном этапе пока что дистанцируется от этой тенденции.

В национальных интересах этого государства построить своё законодательство таким образом, чтобы оно не противоречило (на сколько это возможно) принятым в будущем международным нормам использования ИИ, максимально обойти все положения, которые будут прописаны в контексте запрета использования ИИ в милитаристских целях. Это одна из главных причин, по которым Израиль так откладывает принятие закона об ИИ. Другая причина, конечно же, связана с юридическими сложностями описания ИИ, потому что, ввиду широкого поля использования технологий ИИ, сложно даже дать чёткое полноценное определение самого ИИ. Разумеется, что израильские специалисты ответственно подходят к этому вопросу, анализируя

опыт нормативно-правового регулирования деятельности ИИ в других странах [1].

Заключение. ИИ в Израиле сейчас активно развивается и будет продолжать развиваться, в том числе и в сфере вооружений. Наиболее вероятно, что мировое сообщество не станет этому препятствовать по двум причинам. Во-первых, в сотрудничестве с Израилем в сфере ИИ заинтересованы слишком много государств, поэтому мало кому выгодно вступать в конфронтацию с Израилем касательно этой тематики. Во-вторых, Израиль до сих пор не подписал ДНЯО, к чему мировое сообщество относится компромиссно ввиду специфики региона [9]. Следовательно, есть основания полагать, что к неприсоединению Израиля в договорах об ограничении деятельности ИИ будет аналогичное отношение. Таким образом, на данном этапе Израиль – страна, где ИИ может развиваться с минимальным количеством препятствий и максимально подготовленными для этого условиями.

Список источников и литературы:

1. Афанасьевская А.В. Правовой статус искусственного интеллекта. //Вестник Саратовской государственной юридической академии 2021 г., С. 89.
2. Незнамов А.В. Регулирование искусственного интеллекта в мировой практике // [Электронный ресурс] URL: https://ethics.cdto.ranepa.ru/3_8#link193 (дата обращения: 11.05.2023г.)
3. Савина Н.П., Карпова Е.А. Стартап – экосистема: опыт Израиля. // Международная торговля и торговая политика, 2021 г.
4. Танг Дарен. Резюме Глобальный инновационный индекс — 2022. // Всемирная организация интеллектуально собственности. С.4.
5. Фиговский О. Достижения искусственного интеллекта в Израиле. // АНО "Центр междисциплинарных исследований им. С.П. Курдюмова "Сретенский клуб" 26.11.2021 г. // [Электронный ресурс] URL: https://spkurdyumov.ru/digital_economy/dostizheniya-iskustvennogo-intellekta)-v-izraile/ (дата обращения: 11.05.2023г.)

6. В Европарламенте согласовали закон об искусственном интеллекте. // [Электронный ресурс] URL: https://pravo.ru/news/246436/ (дата обращения: 11.05.2023г.)

7. Запущена национальная программа по продвижению искусственного интеллекта на сумму около 2 млрд. шекелей // [Электронный ресурс] URL: https://www.israeldefense.co.il/node/55208 (дата обращения: 11.05.2023г.)

8. Израиль отказывается от членства в Глобальном соглашении об использовании ИИ в армии — СМИ. // [Электронный ресурс] URL: https://israelan.com/news/izrail-otkazyvaetsya-ot-chlenstva-v/91272 (дата обращения: 11.05.2023г.)

9. Израиль отказался подписывать Договор о нераспространении ядерного оружия. // [Электронный ресурс] URL: https://www.vesti.ru/article/2053348 (дата обращения: 11.05.2023г.)

10. Израильское правительство разрабатывает национальную стратегию, чтобы сделать страну лидером в области искусственного интеллекта. // [Электронный ресурс] URL: https://russiaisrael.ru/en/analitika-page/advertising-campaigns/ (дата обращения: 11.05.2023г.)

11. Оборона Израиля делает ставку на искусственный интеллект // [Электронный ресурс] URL: https://news.rambler.ru/other/45002253/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 11.05.2023г.)

12. Секторальный страновой анализ рынка ИКТ-услуг Израиля // Электронный ресурс] URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://export.nso.ru/sites/export.nso.ru/wodby_files/files/page_1845/izrail_0.pdf (дата обращения: 11.05.2023г.)

13. Mobileye. Основание и раннее руководство. // [Электронный ресурс] URL: https://www.mobileye.com/about/ (дата обращения: 11.05.2023г.

14. Rogerson Annys, Hankins Emma, Nettel Pablo Fuentes, Rahim Sulamaan «Government AI Readiness Index 2022» // Oxford Insights. C.8

[Электронный ресурс] URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf (дата обращения: 11.05.2023г.)

15. Rogerson Annys, Hankins Emma, Nettel Pablo Fuentes, Rahim Sulamaan «Government AI Readiness Index 2022» // Oxford Insights. С.30 [Электронный ресурс] URL:chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf (дата обращения: 11.05.2023г.)

16. MENA Countries 2023 // [Электронный ресурс] URL: https://worldpopulationreview.com/country-rankings/mena-countries (дата обращения: 11.05.2023г.)

17. Cybersecurity powerhouse Israel remains open to hackers // [Электронный ресурс] URL: https://www.al-monitor.com/originals/2022/09/cybersecurity-powerhouse-israel-remains-open-hackers#:~:text=Israel%27s%20leadership%20in%20the%20cyber,investments%20stood%20at%20%248.8%20billion (дата обращения: 11.05.2023г.)

18. Israel Innovation Authority // Электронный ресурс] URL: https://innovationisrael.org.il/en/ (дата обращения: 11.05.2023г.)

19. REAIM 2023 Call to Action. // Government of Netherlands. [Электронный ресурс] URL: https://www.government.nl/documents/publications/2023/02/16/reaim-2023-call-to-action (дата обращения: 11.05.2023г.)

Романов Роман Романович
аспирант, РГГУ
E-mail: roman-romanov-1998@list.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РАБОТЕ ЭКСПЕРТНО-АНАЛИТИЧЕСКИХ ЦЕНТРОВ: ПРИМЕР ПРОГНОЗИРОВАНИЯ

Аннотация. *Данная статья рассматривает применение искусственного интеллекта (ИИ) в экспертно-аналитических центрах для прогнозирования событий в международных отношениях. Объектом особенного интереса в тексте представлены генеративные языковые модели по типу Chat GPT. Применение ИИ в экспертно-аналитических центрах можно рассматривать как решение нескольких важных проблем: нехватка квалифицированного персонала, временные издержки при решении рутинных задач, а также недостаточный уровень финансирования. Это становится особенно актуальным в условиях ускоренной динамики развития международных отношений и частных проблем, таких как риски в информационном пространстве и обновление международной системы.*

Ключевые слова: *искусственный интеллект, прогнозирование, экспертно-аналитическая деятельность.*

Технологии искусственного интеллекта используются во внешнеполитической экспертизе относительно давно. Применение электронно-вычислительных машин (ЭВМ) для организации «военных игр» RAND в 1959 г. – один из нескольких примеров [1]. Появление продвинутых чат-ботов по типу ChatGPT повысило интерес бизнеса, госструктур и некоммерческих организаций к нейросетям и побудило многих из них разработать планы по внедрению ИИ во внутренние процессы. Это имеет значение для экспертно-аналитического сообщества по нескольким причинам. Первая связана с нехваткой квалифицированного персонала. Вторая заключается в экономии времени при использовании нейросети в решении рутинных задач (поиск данных и т.д.). Третья исходит из финансовых

интересов организаций: применение ИИ в отдельных сферах поможет сократить расходы.

Все вышеперечисленное, в свою очередь, связано с более общим и абстрактным фактором: ускоренной динамикой развития международных отношений. Под этим подразумеваются такие частные проблемы, как риски в информационном пространстве и общие, например, обновление международной системы, концептуально новое наполнение норм ее функционирования (отказ от договорно-правовых механизмов времен Холодной войны, смещение экономического потенциала в Азиатско-Тихоокеанский регион (АТР) и решоринг (возвращение производств, ранее перенесенных в страны с более низкими производственными и прочими издержками)).

Главной задачей фабрик мысли является изучение этих процессов. Довольно часто понятие «изучение» путают с анализом, в то время, как анализ – это отдельный метод. Таковым является и прогнозирование – один из наиболее комплексных и интересных методов во внешнеполитической экспертизе. Актуальность выбранной темы можно объяснить двумя факторами:

Во-первых, с учетом повышенной динамики изменений в международной системе оперативное и качественное прогнозирование даже краткосрочных событий стало более комплексной задачей.

Во-вторых, многофакторность современных процессов требует ознакомления со темами, необязательно напрямую связанными с международными отношениями. Нейросеть может с меньшими временными и интеллектуальными затратами интегрировать проблемы из разных областей науки в единую логическую «цепочку» (текст).

Встраивание нейросетей в деятельность центров могло бы сократить временные издержки и улучшить качество материалов. Одновременно с этим, стоит уточнить, что существующие генеративные модели склонны к придумыванию фактов и допускают ошибки при изложении ответов [2].

Заключение. Исходя их этого, цель исследования – продемонстрировать, как использовались ранее и как можно применять в будущем технологии ИИ для прогнозирования событий в международных отношениях, а также выявить наиболее эффективные способы реализации подобных задач. В работе используются исторические и политологические методы: историко-генетический подход, институциональный подход и многофакторный анализ.

Список источников и литературы:

1. Диксон П. Фабрики мысли / П. Диксон. – М.: ООО «Издательство АСТ», 2004.

2. Jensen K. T. Yes, Machines Make Mistakes: The 10 Biggest Flaws In Generative AI // PCmag // URL: https://uk.pcmag.com/news/146481/yes-machines-make-mistakes-the-10-biggest-flaws-in-generative-ai

Тимофеева Анастасия Юрьевна
руководитель международного направления
ФГБУ «НИИ «Интеграл», Москва
E-mail: nasty-timofeeva2000@mail.ru

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТЕХНОЛОГИЯХ СОЗДАНИЯ «ДИПФЕЙКОВ» КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В данной статье рассматривается проблема использования искусственного интеллекта для создания и распространения негативного медиаконтента. Особое внимание уделено такому явлению как «дипфейки» и их применения не только в целях, получения экономической выгоды, но и для манипулирования общественным сознанием на национальном и межнациональном уровнях. В статье анализируется негативное влияние искусственного интеллекта — как инструмента для разжигания внутриполитических и международных конфликтов. Актуальность данной проблемы обусловлена необходимостью понимания всех рисков, которые несёт развитие цифровых технологий в сфере разработки самообучающихся программ на базе нейросетей искусственного интеллекта.*

Ключевые слова: *искусственный интеллект, «дипфейк», кибер-риски, информационные технологии, информационная безопасность.*

В настоящее время во всем мире отмечается тенденция использования искусственного интеллекта (ИИ) для создания и распространения негативной информации с целью влияния на общественное мнение, например, в рамках политического дискурса – в пределах государства, или разжигания международных конфликтов – на глобальном уровне. Новейшие программы и широкое распространение машинного обучения упростили процесс создания фальшивых, дискредитирующих личность видео и медиа-материалов – «дипфейков» [1].

Уже в ближайшем будущем «дипфейки» могут затронуть различные уровни общественной и политической жизни и способствовать

распространению широкого спектра угроз: от репутационных рисков для обычного человека, до развития организованной преступности и проблем социальной стабильности и национальной безопасности.

Серьезные опасения вызывает возможность использования «дипфейков» для разжигания конфликтов, массовых гражданских беспорядков и подрыва национальной безопасности – применение такой технологии может спровоцировать межэтнические или межконфессиональные столкновения.

Развитие программных средств обработки «больших данных», увеличение быстродействия вычислительных средств, опережающие разработки ИИ ставят на повестку дня и проблему воздействия «дипфейков» при помощи различных психологических инструментов на массовую аудиторию.

В настоящее время на рынке информационной безопасности отсутствуют специальные технологии и решения для эффективной защиты от «дипфейков». Тем не менее, определённая деятельность на данном направлении ведется.

В США, в частности, реализуется ряд программ по противодействию информационным угрозам и манипуляциям в средствах массовой информации. Основными из них являются SemaFor (Semantic Forensics – программа экспертизы содержания мультимедийных материалов, предназначенная для автоматизированного поиска фальсифицированных медиаматериалов и защиты от крупномасштабных дезинформационных атак в режиме реального времени) и MediFor (Media Forensics – проект по экспертизе средств массовой коммуникации для выявления недостоверных видео, сопровождаемых ложной аудиозаписью, и позволяющий получить цифровой, физический и семантической индикаторы целостности) [2].

Одновременно с программами противодействия информационным угрозам и манипуляциям в средствах массовой информации, в последнее время со стороны Министерства обороны США просматривается тенденция использования дипфейк-технологий в качестве информационного оружия. Об этом свидетельствует анализ запроса коммерческих предложений (Request for

proposal) Командования специальными операциями США (Special Operations Command - SOCOM) с перечнем необходимых устройств и технологий, опубликованного в феврале 2023 года на официальном веб-сайте управления госзаказами Правительства США (www.sam.gov) [3].

Заключение контрактов с частным бизнесом на разработку и производство устройств, систем, программного обеспечения и т.п. военной направленности для министерства обороны США является стандартной процедурой. Однако, данном случае, уникальность ситуации заключается в том, что правительство страны через документы в открытом доступе заявляет о своём намерении внедрить дипфейк-технологии для ведения интернет-пропаганды и организации дезинформационных онлайн-кампаний, направленных на иностранные государства.

В частности, в разделе «Передовые технологии для использования в операциях военной информационной поддержки (MISO)» указано: «Предоставить следующее поколение технологий создания «дипфеков» или других подобных технологий для генерации информационных сообщений и проведения информационных операций через нетрадиционные каналы (соцсети) в соответствующих децентрализованных/частично децентрализованных узлах. Требуется создание систем следующего поколения для «захвата» устройств Интернета вещей (IoT), направленных на сбор данных о местном населении, мониторинг уровня популярности и эффективности запущенных фейковых сообщений и получение обратной связи, путем фильтрации полученных данных». Это позволит MISO создавать и продвигать сообщения, которые могут быть с большей готовностью восприняты сообществом в соответствующей информационной среде». [3]

Проведение подобных спецопераций предполагает внедрение шпионских программ, в том числе, для мониторинга успешности проведения информационных кампаний, а также для распространения дезинформации и дипфейков, направленных, на политических и/или военных лидеров

иностранных государств с целью формирования к ним недоверия среди местного населения.

Командования спецоперациями США планирует получить усовершенствованные средства для проведения операций информационного влияния, кибер-атак, нарушения связи противника и осуществление кампаний по дезинформации на тактическом и оперативном уровнях. Ведомство ищет возможность приобретения технологий следующего поколения для сбора разрозненных данных через общедоступные и открытые источники, такие как социальные сети, местные СМИ и т.д. [4].

Рассматривается также получение от частных компаний предложений по разработке высококачественного ПО, систем и технологических концепций, связанных с данной темой для использования в «операциях военной информационной поддержки».

Кроме того, в своем запросе SOCOM объявило о наборе высококлассных специалистов для отслеживания повседневных разговоров и переписки иностранных граждан, создания целевой пропаганды, антирекламы, распространения дипфейков [4,5].

В рамках обеспечения национальной безопасности правительство США через свои военные ведомства активно использует новые технологий на основе ИИ не только для отслеживания кибер-рисков и противодействия кибер-атакам, но в тоже время намерено использовать деструктивное информационно-психологическое воздействие дипфейк-технологий против граждан других государств [4,5].

Налицо тенденция, когда технологии ИИ, создаваемые в целях ускорения технологического прогресса, становятся оружием против общества на государственном уровне.

Заключение. Таким образом, злонамеренное использование технологий на основе ИИ представляет собой значительные угрозы информационной безопасности и может спровоцировать или обострить межнациональные,

межэтнические и межконфессиональные противоречия, а также стать причиной дестабилизации экономической и политической ситуации отдельных государств и целых регионов. Одним из возможных решений этой проблемы является формирование международной нормативно-правовой базы по регулированию применения технологии ИИ, в том числе для запрета ее использования в целях деструктивного информационно-психологического воздействия.

Список источников и литературы:

1. Дипфейк - методика компьютерного синтеза изображения, основанная на искусственном интеллекте, которая используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики, образовалось от сочетания терминов «глубокое обучение» (англ. deep learning) и «подделка» (англ. fake). Иванов В.Г., Игнатовский Я.Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. Т. 7. № 4. С. 379–386. DOI: 10.22363/2312-8313-2020-7-4-379-386

2. Программы Агентства перспективных исследований в области обороны США по Анализу информации // Центр стратегических оценок и прогнозов в области обороны США по Анализу информации [Официальный сайт] URL:https://csef.ru/ru/nauka-i-obshchestvo/445/programmy-agentstva-perspektivnyh-issledovanij-v-oblasti-oborony-ssha-po-analizu-informaczii-9381?ysclid=ljh886qs4t220399944 (дата обращения 28.04.2023)

3. Special operations forces acquisition, technology, and logistics directorate of science and technology (SOF AT&L-ST) broad agency announcement USSOCOM-BAAST-2020, Amendment 3 for technology development and advanced technology development// Military Information Support Operations (MISO) 4.3.1.4// The Official U.S. Government System for Contract Opportunities [Official website] URL:

https://sam.gov/opp/bf402ee8c98a4998adbe789c878e1098/view (дата обращения 28.04.2023)

4. US Special Forces Looking to Tap Deepfake Tech to Influence Foreign Populations// Farsnews Agency [Web source] URL: https://www.farsnews.ir/en/news/14011217000202/Repr-US-Special-Frces-Lking-Tap-Deepfake-Tech-Inflence-Freign (дата обращения 28.04.2023)

5. US military group wants weaponized deepfakes, better biometric tools // BiometricUpdate.com by the Biometrics Research Group, Inc. // [Web source] URL: https://www.biometricupdate.com/202303/us-military-group-wants-weaponized-deepfakes-better-biometric-tools (дата обращения 28.04.2023)

Трофимова Ольга Сергеевна
Национальный центр управления обороной Российской Федерации
старший переводчик
E-mail: trofi.fff@gmail.com

МОРАЛЬНО-ЭТИЧЕСКИЙ АСПЕКТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *Статья посвящена изучению морально-этического аспекта искусственного интеллекта и построена по принципу представления различных позиций по перечню аспектов проблемы правосубъектности систем искусственного интеллекта.*

Ключевые слова: *искусственный интеллект, правосубъектность, этика, электронное лицо, юридическое лицо.*

Проблема ответственности в академических научных исследованиях. Проблема распределения ответственности за функционирование технологических решений на основе искусственного интеллекта (далее - ИИ) является наиболее значимой и обсуждаемой в исследованиях этики ИИ. От ее решения во многом зависит определение правового статуса объектов систем на основе сильного ИИ и охраноспособности результатов интеллектуальной деятельности (РИД), созданных с использованием ИИ. Для обзора были отобраны источники, в которых демонстрируются различные подходы к проблеме определения ответственности за решения ИИ. Важным остается тот факт, что решение проблемы возможно только усилиями специалистов из разных областей знания и деятельности.

Одним из основных авторитетных исследователей проблемы ответственности в контексте работы систем ИИ является профессор философии технологии и медиа философского факультета Венского университета Марк Кокельберг, автор монографии «Этика искусственного интеллекта» («AI Ethics»). Разработка проблематики начинается с

определения критериев, необходимых для приписывания кому-либо ответственности посредством ссылки на классическую работу Аристотеля «Никомахова этика». Проблема в ответственности в контексте функционирования ИИ возникает в силу того, что ИИ может совершать действия с этическими последствиями и не осознавать при этом, что он делает, будучи вне морального мышления. Следовательно, он не может быть агентом моральной ответственности, так как у него нет сознания, свободы воли, эмоций, способности формировать намерения и т.д.

Ключевых элементов концепции М.Кокельберга два: идея ответственности и идея распределенной ответственности. Что касается, идеи ответственности, то, во-первых, ИИ может совершать действия и принимать решения, но ответственность за них несут только люди. Во-вторых, ИИ не может быть ответственным и поэтому не может быть безответственным [3]. Следовательно, люди должны нести ответственность за то, что они делают и решают при разработке или использовании ИИ в силу того, что они удовлетворяют классическим условиям моральной агентности, в отличие от ИИ. Такое решение сталкивается с несколькими проблемами. Первая из них – превышение отдельных когнитивных способностей человека, критически значимых в сфере принятия решений, технологии ИИ. Как следствие, люди не всегда успевают принять меры для корректировки решений ИИ, особенно в экстренных ситуациях. Это может приводить к возникновению «пробелов в ответственности» (responsibility gap): полного или частичного отсутствия контроля человека над автономными технологиями ИИ, являющимися причиной невозможности прямого атрибутирования ответственности тому или иному лицу.

Возложить ответственность за действия технологий можно и на разработчиков, и на пользователей ИИ. В этом и есть идея распределенной ответственности. Таким образом, будет существовать «корпоративная ответственность» [4]. Альтернативой обозначенному выше подходу к решению проблемы ответственности посредством ее переноса исключительно

на людей является подход, допускающий возможность переноса ответственности на саму технологию. Данная точка зрения на проблему не является популярной, но содержит ряд интересных положений.

Правосубъектность систем ИИ. Система ИИ – субъект или объект права? На сегодняшний день в юридической практике общепринятым является отношение к системе ИИ как к объекту, по поводу которого (а не у которого) возникают права и обязанности. Однако все шире ведется академическая и общественная дискуссия о необходимости признания возможности таких систем являться носителями субъективных прав и юридических обязанностей. Только осенью 2021 года в РФ были проведены три тематические сессии обсуждения статуса ИИ: международный форум «Этика ИИ: начало доверия» [5], международная онлайн-конференция «AI Journey» [4], конференция на базе Высшей школы экономики «Мир людей и машин: этические и правовые аспекты цифровой трансформации» [2].

Проблема юридической ответственности систем ИИ. Одним из наиболее главных является вопрос правовой ответственности за вред, причиненный действиями автономной системы, действующей на основе ИИ.

Управляющий партнер петербургского филиала юридической фирмы «Дэнтонс» («Dentons»), разработавшей первый в России законопроект о робототехнике [1], В.Б. Наумов и советник фирмы В.В.Архипов в своей работе отмечают, что проблема ответственности, как правило, является отправной точкой исследований, посвященных юридической стороне использования роботов [1]. Более того, именно эта сторона вопроса подчеркнута в нашумевшей резолюции Европейского парламента от 16 февраля 2017 года с рекомендациями Комиссии по нормам гражданского права, касающимся робототехники (Commission on Civil Law Rules on Robotics) [9]. В качестве возможного решения резолюция предлагает рассмотреть создание в долгосрочной перспективе особого правового статуса роботов, чтобы, как минимум, наиболее сложные (sophisticated) автономные роботы могли быть наделены статусом «электронного лица», ответственного за возмещение

любого ущерба, который оно может причинить. Однако стоит отметить, что данная идея «электронного лица» не получила развития к текущему моменту.

Один из ведущих российских исследователей тематики правового регулирования ИИ П.М. Морхат полагает, что предоставление правосубъектности системам ИИ оправдано с точки зрения решения целого ряда правовых проблем, таких как, например, освобождение создателей и пользователей таких систем от ответственности за их автономное поведение, а также для решения проблем, связанных с ведением электронного бизнеса и вопросами принадлежности РИД, создаваемых ИИ [6]. В другой своей работе автор высказывает позицию, что наделение системы ИИ правовым статусом «электронного лица» должно осуществляться не в целях освобождения физических и юридических лиц от ответственности, а, напротив, должно быть направлено на решение проблемы идентификации и подотчетности «юнитов» ИИ и стоящих за ними реальных людей [6].

Правосубъектность систем ИИ, аналогичная статусу юридического лица. П.М. Морхат справедливо отмечает, что принципиальным сходством так называемого электронного лица с лицом юридическим является то, что и первое, и второе существуют не сами по себе, а являются средством достижения их фактическими владельцами определенных целей и создаются исключительно в их интересах [6]. Продолжая эту логику, судья Конституционного Суда Российской Федерации Г.А. Гаджиев и правовед Е.А. Войниканис в совместной работе задаются вопросом (риторического характера): нельзя ли удовлетворить общественную потребность в признании правовой личности роботов (которая может возникнуть в связи с совершенствованием технологий ИИ) путем признания их особой разновидностью юридических лиц [3].

Степень разработанности этой концепции подтверждается тем, что именно она нашла отражение в законопроекте о робототехнике (первом в российской практике), разработанном международной фирмой «Дэнтонс» («Dentons») по заказу компании «Гришин Роботикс» («Grishin Robotics»).

Заключение. В результате анализа вышеуказанных источников были выявлены следующие наиболее распространенные проблемы, связанные с распределением ответственности за функционирование технических решений ИИ:

- определение и переопределение моральной ответственности;

- условия необходимые для приписывания моральной ответственности: контроль и знание, объяснимость и прозрачность, автономность, наличие намерений;

- определение типов моральных агентов, несущих ответственность в текущей парадигме – люди – агенты: разработчики ИИ; компания, разрабатывающая ИИ; клиенты; поставщики данных; эксперты, размечающие данные; государство (законодатель); составители этических рекомендаций; корпоративный менеджмент;

- проблема «многих рук» и «многих объектов»;

- проблема доверия и надежности: недостаточное и чрезмерное;

- определение допустимой степени автономности ИИ.

Список источников и литературы:

1. Архипов В.В., Наумов, В.Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности. Закон № 5. 2017. (доступ из системы «КонсультантПлюс»)

2. Всероссийская научная онлайн-конференция «Мир людей и машин: этические и правовые аспекты цифровой трансформации». – URL: https://digitallaw.hse.ru/digitalethics2021/ (дата обращения: 05.05.2023).

3. Гаджиев Г.А., Войниканис Е.А. Может ли робот быть субъектом права? (поиск правовых форм для регулирования цифровой экономики). Правовая мысль и современность. – URL: https://cyberleninka.ru/article/n/mozhet-li-robot-byt-subektom-prava-poisk-pravovyh-form-dlya-regulirovaniya-tsifrovoy-ekonomiki?ysclid=ljlilyhf3e119840370 (дата обращения: 05.05.2023).

4. Конференция Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века». – URL: http:// kremlin.ru/events/president/news/64545 (дата обращения: 05.12.2022).

5. Международный форум «Этика искусственного интеллекта: начало доверия». – URL: https://ac.gov.ru/news/events/page/i-mezdunarodnyj-forum-etika-iskusstvennogo-intellekta-nacalo-doveria-26602 (дата обращения: 05.05.2023).

6. Морхат П.М. Юнит искусственного интеллекта как электронное лицо. Вестник Московского государственного областного университета. Серия: Юриспруденция. №2, 2018, стр. 61-73.

7. Coeckelbergh M. AI Ethics. Cambridge, Massachusetts, USA: The MIT Press, 2020

8. Coeckelbergh M. “Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability”. Science and engineering ethics vol. 26,4 (2020): 2051 – 2068.

9. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), subparagraph (f) of paragraph 59 (URL: https://www.europar1.europa.eu/doceo/document/TA-8-2017-0051_EN.pdf)

Чичерина Карина Сергеевна
ассистент
Южный федеральный университет, Институт компьютерных технологий
и информационной безопасности
E-mail: kchicherina@sfedu.ru

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И АНАЛИЗА ДАННЫХ В СИСТЕМЕ ОБНАРУЖЕНИЯ ФИШИНГА И СПАМА

Аннотация. *В статье планируется рассмотреть практические примеры использования системы обнаружения фишинга и спама на основе искусственного интеллекта, чтобы показать ее эффективность в реальном мире. А именно, обзор некоторых примеров скриптов для обнаружения фишинга и спама на языке Python.*

Ключевые слова*: алгоритм распознавания текста, фишинг, спам, безопасность, машинное обучение, Python.*

Введение. Методы машинного обучения представляют собой мощный инструмент для борьбы с фишингом и спамом. Фишинг и спам являются распространенными проблемами в онлайн-среде, и они могут нанести значительный ущерб как индивидуальным пользователям, так и организациям [2].

Машинное обучение позволяет анализировать большие объемы данных и обнаруживать характерные признаки, которые указывают на наличие фишинговых попыток или спама [2]. С помощью алгоритмов машинного обучения можно создать модели, которые автоматически классифицируют электронные письма, сообщения или веб-страницы как потенциально опасные или нежелательные.

Обзор методов машинного обучения. Некоторые из популярных методов машинного обучения, которые применяются для борьбы с фишингом и спамом, включают:

1. Классификация на основе признаков: Алгоритмы машинного обучения могут обучаться на основе набора характеристик электронных писем или сообщений, таких как заголовки, содержание, адреса отправителей и прочие признаки, чтобы определить, являются ли они фишинговыми или спамовыми [2].

2. Анализ контента: Методы машинного обучения могут быть использованы для анализа содержимого электронных писем, сообщений или веб-страниц, чтобы выявить подозрительные или нежелательные элементы. Например, можно искать ключевые слова, фразы или структуры, которые часто встречаются в фишинговых или спамовых сообщениях [8].

3. Обнаружение аномалий: Машинное обучение может быть применено для создания моделей, которые научатся распознавать аномальное поведение, связанное с фишингом или спамом. Это позволяет выявлять новые, ранее неизвестные виды атак и адаптироваться к изменяющимся методам злоумышленников.

4. Анализ поведения: Методы машинного обучения могут отслеживать и анализировать поведение пользователей, чтобы выявлять подозрительные активности, связанные с фишингом или спамом. Например, можно анализировать частоту неправильных попыток входа или использование неподозрительных доменных имен в электронных адресах отправителей. Этот подход основан на том, что злоумышленники могут использовать определенные схемы или поведенческие паттерны, которые могут быть обнаружены с помощью алгоритмов машинного обучения [7].

Обзор технологий распознавания фишинга и спама. В системах обнаружения фишинговых атак и спама используются различные методы машинного обучения и анализа данных, такие как:

Классификация: Метод классификации является основным методом, используемым в системах обнаружения фишинга и спама. Для классификации используются алгоритмы машинного обучения, такие как деревья решений,

метод k-ближайших соседей, логистическая регрессия, метод опорных векторов и наивный байесовский классификатор [1, 3].

Обработка естественного языка (Natural Language Processing, NLP): Обработка естественного языка используется для анализа текстов, используемых в электронной почте и на веб-сайтах, чтобы определить, содержит ли текст признаки фишинга или спама. NLP-методы включают анализ тональности, анализ эмоций и анализ ключевых слов [5].

Анализ контента: Анализ контента используется для обнаружения фишинговых сайтов и веб-страниц. Для этого используются алгоритмы, которые анализируют HTML-код веб-страницы, чтобы определить наличие фишинговых признаков, таких как поддельные формы входа в систему [4].

Кластеризация: Кластеризация используется для группировки электронных писем по сходству в содержании и/или отправителям. Это позволяет выделить фишинговые письма и спам, а также отслеживать их источники.

Практические примеры реализации. Далее планируется рассмотреть практические примеры использования системы обнаружения фишинга и спама на основе методов машинного обучения и спама тивность на языке Python. А именно, обзор некоторых примеров скриптов, с применением библиотеки для анализа данных Pandas и более простое приложение [9].

Данный код демонстрирует применение алгоритма случайного леса (Random Forest)[10] для классификации электронных писем на фишинговые и нежелательные:

```
import pandas as pd
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
# Загрузка данных
data = pd.read_csv('файл_с_данными.csv')
# Подготовка данных
```

```
vectorizer = CountVectorizer()
X = vectorizer.fit_transform(data['содержание_писем'])
y = data['метки']  # 1 для фишинга, 0 для нежелательных
# Разделение данных на обучающую и тестовую выборки
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
# Создание и обучение модели случайного леса
model = RandomForestClassifier()
model.fit(X_train, y_train)
# Оценка точности модели
accuracy = model.score(X_test, y_test)
print(f'Точность модели: {accuracy}')
# Пример классификации нового письма
new_email = ['Здравствуйте, это ваш банк. Пожалуйста, подтвердите свои данные.']
new_email_transformed = vectorizer.transform(new_email)
prediction = model.predict(new_email_transformed)
print(f'Классификация нового письма: {prediction}')
```

В этом примере кода мы используем библиотеки Pandas для загрузки данных из файла CSV, CountVectorizer для преобразования текстовых данных писем в числовые признаки, RandomForestClassifier для создания модели случайного леса, а также train_test_split для разделения данных на обучающую и тестовую выборки [10].

После обучения модели мы оцениваем ее точность на тестовой выборке и выводим результат классификации нового письма, передавая его через преобразованный CountVectorizer и вызывая метод predict модели.

Ниже приведем пример более простой реализации:

```
import re
def is_phishing_or_spam(email_text):
 # Определяем тип сообщения по наличию ключевых слов в тексте
```

phishing_keywords = ['аккаунт', 'войти', 'подтвердить', 'безопасность', 'блокировка', 'пароль']

spam_keywords = ['реклама', 'скидка', 'акция','акции', 'выгодно', 'деньги']

for keyword in phishing_keywords:

if re.search(keyword, email_text, re.IGNORECASE):

return 'Этот текст может содержать фишинговые атаки'

for keyword in spam_keywords:

if re.search(keyword, email_text, re.IGNORECASE):

return 'Spam'

return 'Это письмо не содержит угроз'

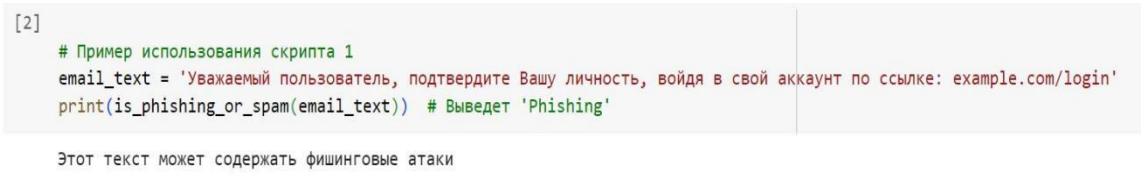


Рис. 1. Пример использования скрипта.

Эти работы описывают различные подходы и методы, которые могут использоваться для создания систем обнаружения фишинга и спама на основе машинного обучения и анализа данных [6].

Заключение. В заключение хочется отметить, что методы машинного обучения представляют мощный инструмент для защиты от фишинга и спама в онлайн-среде. Алгоритмы машинного обучения позволяют анализировать большие объемы данных, выявлять характерные признаки и обнаруживать подозрительные активности, связанные с фишинговыми атаками и спамом.

Однако следует отметить, что злоумышленники постоянно разрабатывают новые методы атак, поэтому необходимо постоянно совершенствовать и адаптировать модели машинного обучения, чтобы быть впереди в непрекращающейся борьбе со злоумышленниками. Кроме того, машинное обучение должно использоваться в сочетании с другими методами защиты, такими как обновление программного обеспечения, обучение

пользователей и регулярная проверка безопасности, чтобы обеспечить полноценную защиту от фишинга и спама.

В целом, методы машинного обучения предоставляют эффективные инструменты для борьбы с фишингом и спамом, обеспечивая автоматическое обнаружение и фильтрацию подозрительных или вредоносных сообщений. Использование этих методов позволяет снизить угрозу и ущерб, связанные с фишингом и спамом, и создать более безопасную онлайн-среду для пользователей и организаций.

Список источников и литературы:

1. Нейман И. Математические основы квантовой механики. // М.: «Наука», 1964.
2. Николенко С.И., Кадурин А.А., Архангельская Е.О. Глубокое обучение. - С.-Петербург: Изд-во Питер, 2017. - 480 с.
3. Хайкин С. Нейронные сети: полный курс, 2-е издание. - Издательский дом Вильямс, 2008.
4. Das, Ashwin, and Benny Thomas. Natural Language Processing with Python and NLTK: Analyzing Text with the Natural Language Toolkit.
5. D. Zakharyan, G. Tsirunyan, A. Abrahamyan, E. Sukiasyan. Phishing Detection using Machine Learning Techniques - International Journal of Advanced Computer Science and Applications, 2019.
6. Bird S., Klein E., and Loper E. "Natural Language Processing in Python: Analyzing Text with the Natural Language Toolkit." O'Reilly Media, 2020.
7. Metz C. The rise of the artificially intelligent hedge fund. // January 2016.
8. Hyannis, MA, USA. Sarkar, Dipanjan. "Text Analytics with Python: A Practical Real-World Approach to Gaining Actionable Insights from your Data." Apress, 2020.
9. Pandas, Python. Available at: https://pandas.pydata.org/
10. Scikit-learn, Python. Available at: https://scikit-learn.org/stable/.

Научное издание

БЮЛЛЕТЕНЬ
I МЕЖДУНАРОДНОЙ МОЛОДЕЖНОЙ КОНФЕРЕНЦИИ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник тезисов

Научный руководитель:
Яковенко Александр Владимирович
(доктор юридических наук, профессор)

Рецензенты:
Данельян Андрей Андреевич,
(доктор юридических наук, профессор)
Карпович Олег Геннадьевич,
(доктор юридических наук, доктор политических наук, профессор)
Крамаренко Александр Михайлович

Ответственные редакторы:
А.Ж. Мартиросян, Р.Н. Шангараев (доктор политических наук)