**Федеральное государственное бюджетное образовательное учреждение высшего образования «Дипломатическая академия Министерства иностранных дел Российской Федерации»**

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

**Направление подготовки:** 38.04.04. Государственное и муниципальное управление
**Направленность**: Гибридные войны: технологии управления и безопасность
**Форма обучения:** очная
**Квалификация выпускника:** магистр
**Объем дисциплины:**
в зачетных единицах: 4 з.е.
в академических часах: 144 ак. ч.

2025

Карпович О.Г. Защита критической инфраструктуры: Рабочая программа дисциплины: Москва: Дипломатическая академия МИД России, 2025 г.
Рабочая программа по дисциплине: «Защита критической инфраструктуры» по направлению подготовки в магистратуре 38.04.04 Государственное и муниципальное управление, направленность «Гибридные войны: технологии управления и безопасность», составлена Карповичем О.Г. в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 13.08.2020 года № 1000, зарегистрированного в Министерстве юстиции Российской Федерации 28.08.2020 г. № 59530.

Руководитель ОПОП Карпович О.Г.

Директор библиотеки Толкачева Ю.В.

Рабочая программа:

**обсуждена и рекомендована** к утверждению решением кафедры
от 24 января 2025 г., протокол № 21
Заведующий кафедрой
стратегических коммуникаций
и государственного управления Карпович О.Г.

**рекомендована**
Учебно-методическим советом (УМС) Академии
от 20 марта 2025 г., протокол № 6
Председатель УМС Ткаченко М.Ф.

**одобрена** Ученым Советом Академии 26 марта 2025 г., протокол № 4

## 1. Цели и задачи освоения дисциплины (модуля)

**Целью** дисциплины является освоение базовых технологий защиты критической инфраструктуры путем изучения теоретико-методологических и прикладных знаний о критической инфраструктуре (КИ) как объекту обеспечения безопасности.
**Задачи** освоения дисциплины:
- сформировать представление о теоретико-методологических основах определения критической инфраструктуры;
- выработать навыки анализа уязвимостей, рисков, угроз объектам КИ;
- развить навык систематизации и определения основных приемов обеспечения безопасности объектов КИ;
- -освоить базовые технологии защиты КИ.

## 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение дисциплины «Защита критической инфраструктуры» направлено на формирование следующих компетенций: УК-1.1; УК-1.2; УК-6.1; УК-6.2; ПК-5.1; ПК-5.2; ПК-5.3

| № п/п | Формируемые компетенции (код и наименование компетенции) | Код и формулировка индикатора компетенции | Планируемые результаты обучения |
|---|---|---|---|
| 1 | **УК-1.1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | **УК-1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними | **Знает** методику постановки цели и определения способов ее достижения<br>**Умеет** определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов, осуществлять сбор, систематизацию и критический анализинформации,необходимой длявыработкистратегиидействий поразрешению проблемной ситуации |
| | | **УК-1.2** Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов | **Знает** проблемную ситуацию как систему, выявляя ее составляющие и связи между ними<br>**Умеет** проводить оценку адекватности и достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников**,** осуществлять поиск решений |

| | | | |
|---|---|---|---|
| | | | проблемной ситуации на основе действий, эксперимента и опыта, критически оценивать возможные варианты решения проблемной ситуации на основе анализа причинно-следственных связей. |
| **2** | **УК-6**. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки | **УК-6.1.** Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует | **Знает**: основные принципы мотивации и стимулирования карьерного развития, способы самооценки и самоопределения<br>**Умеет:** оценить возможности реализации собственных профессиональных целей и расставить приоритеты |
| | | **УК-6.2**. Определяет образовательные потребности и способы совершенствования собственной (в том числе профессиональной) деятельности на основе самооценки | **Знает:** особенности деятельностного подхода в исследовании личностного развития.<br>**Умеет**: провести анализ результатов своей социальной и профессиональной деятельности**,** корректировать планы личного и профессионального развития |
| **3** | **ПК-5** Способен ориентироваться в особенностях аналитического и информационного сопровождения военных, гуманитарных и иных операций, применения политических и информационных технологий, в том числе стратегических коммуникаций, и противодействия им | **ПК-5.1.** Выделяет уровни и виды планирования, организации и проведения информационного сопровождения военных, гуманитарных и иных операций | **Знает** основополагающие международно-правовые документы, определяющие порядок информационного сопровождения военных, гуманитарных и иных операций;<br>**Умеет** характеризовать значение международно-правовых документов, касающихся применения политических и информационных технологий и противодействия им |
| | | **ПК-5.2.** Определяет эффективность организации и проведения информационных | **Знает** инструменты и механизмы проведения информационных кампаний и противодействия им; |

| | | | |
|---|---|---|---|
| | | кампаний, в том числе стратегических коммуникаций, и противодействия им | **Умеет** определять черты различных информационных кампаний и противодействия им; |
| | | **ПК-5.3** Владеет навыками вычленения военных, экономических и политических факторов формирования и реализации современных политических и информационных технологий и противодействия им. | **Знает** специфику политизации и технологизации современного информационного поля<br>**Умеет** анализировать как целостные стратегии информационного воздействия, так и отдельные продукты и элементы массированных информационных кампаний, а также разрабатывать симметричные и ассиметричные информационные и ментальные антидоты |

## 3. Объем дисциплины (модуля) и виды учебной работы

*Очная форма обучения*

| Виды учебной деятельности | | Всего | По семестрам | | | |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 1. Контактная работа обучающихся с преподавателем***: | | 26,3 | | | 26,3 | |
| Аудиторные занятия, часов всего, в том числе: | | 26 | | | 26 | |
| • занятия лекционного типа | | 10 | | | 10 | |
| • занятия семинарского типа: | | 16 | | | 16 | |
| практические занятия | | - | | | | |
| лабораторные занятия | | - | | | | |
| в том числе занятия в интерактивных формах | | | | | | |
| в том числе занятия в форме практической подготовки | | - | | | - | |
| Контактные часы на аттестацию в период экзаменационных сессий - | | 0,3 | | | 0,3 | |
| 2. Самостоятельная работа студентов****, всего | | 117,7 | | | 117,7 | |
| • курсовая работа (проект) | | - | | | - | |
| Подготовка выступлений на семинарских занятиях с презентациями | | 40 | | | 40 | |
| освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы | | 50 | | | 50 | |
| изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | | 27,7 | | | 27,7 | |
| 3.Промежуточная аттестация:<br>зачет | | зачет | | | зачет | |
| ИТОГО:<br>Общая трудоемкость | Ак.часов | 144 | | | 144 | |
| | зач. ед. | 4 | | | 4 | |

## 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

**4.1. Содержание дисциплины «Защита критической инфраструктуры»**

**Тема 1. Понятийный аппарат в области защиты критической инфраструктуры (КИ)** (субъект и объект критической инфраструктуры, автоматизированная система управления, безопасность КИ, государственная тайна, государственная информационная система, гриф секретности, доступ к информации, доступность информации, информационно-телекоммуникационная сеть, инцидент информационной безопасности, компьютерный инцидент, компьютерная атака, критической информационной инфраструктуры (КИИ), конфиденциальность информации и т.д.)

**Тема 2. Классификация объектов КИ, регламенты обеспечения их безопасности и защиты.** Энергетика и коммунальные услуги: поставщики электроэнергии; нефть и газ; поставки угля, природного газа; мазут для дома; поставки для АЗС; поставщики альтернативной энергии (ветровой, солнечной, другой). Информационно-коммуникационные технологии: средства вещания; телекоммуникационные провайдеры (стационарные, сотовые телефоны, интернет, Wi-Fi); Почтовые услуги; Финансы: банковские услуги, государственные департаменты финансов / помощи; налогообложение Здоровье: Программы общественного здравоохранения и оздоровления, помещения больниц / клиник; кровь и продукты крови Продукты питания: цепочки поставок продуктов питания; продовольственные инспекторы; программы импорта / экспорта; продуктовые магазины; Сельскохозяйственная культура; фермерские рынки. Вода: Водоснабжение и охрана; управление сточными водами; программы рыболовства и защиты океана. Транспорт: дороги, мосты, железные дороги, авиация / аэропорты; судоходство и порты; транзит. Безопасность: службы экстренного реагирования; программы общественной безопасности. Правительство: Военное; Преемственность управления.

Сектора КИ: химическая промышленность, коммерческие объекты, коммуникации, критическое производство, плотины, оборонно-промышленная база, аварийные службы, энергетика, финансовые услуги, продовольствие и сельское хозяйство, государственные объекты, здравоохранение и общественное оздоровление, информационные технологии, ядерные реакторы, материалы и отходы, транспортные системы, системы водоснабжения и канализации.

**Тема 3. Нарушители в отношении объектов критической инфраструктуры** (классификация по оснащенности, знаниям, мотивации).

**Тема 4. Защита критической информационной инфраструктуры.** Методики определения угроз безопасности информации в информационных системах.

**Тема 5. Критические для обеспечения обороны страны, безопасности государства и правопорядка процессы**: управленческие, технологические, производственные, финансово-экономические. Механизмы их корректировки, нейтрализации и перезапуска. Технология стресс-тестирования (Предварительная оценка контекста риска и контекста опасности, собственно стресс-тест, принятие решения по стратегии снижения рисков, отчет с рекомендациями по снижению рисков).

*Очная форма обучения*

| № | Раздел дисциплины, тема | Занятия лекционного типа | Практические занятия | Лабораторные работы | Самостоятельная работа |
|---|---|---|---|---|---|
| | | ак.час. | ак.час. | ак.час. | ак.час. |
| 1 | Понятийный аппарат в области защиты критической инфраструктуры (КИ) | 2 | 4 | | 26 |
| 2 | Классификация объектов КИ, регламенты обеспечения их безопасности и защиты. | 2 | 2 | | 13 |
| 3 | Нарушители в отношении объектов критической инфраструктуры | 2 | 4 | | 26 |
| 4 | Защита критической информационной инфраструктуры. | 2 | 2 | | 13 |
| 5 | Критические для обеспечения обороны страны, безопасности государства и правопорядка процессы | 2 | 4 | | 39,7 |
| **ИТОГО** | | **10** | **16** | | **117,7** |

**4.2. Самостоятельное изучение обучающимися разделов дисциплины «**Защита критической инфраструктуры**»**

*Очная форма обучения*

| Вопросы, выносимые на самостоятельное изучение | Формы самостоятельной работы* | Оценочное средство для проверки выполнения самостоятельной работы |
|---|---|---|
| Понятийный аппарат в области защиты критической инфраструктуры (КИ) | Подготовка выступлений на семинарских занятиях с презентациями<br>освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы<br>изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | Выступление на семинарском занятии с презентацией |

| | | |
|---|---|---|
| Классификация объектов КИ, регламенты обеспечения их безопасности и защиты. | Подготовка выступлений на семинарских занятиях с презентациями<br>освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы<br>изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | Выступление на семинарском занятии с презентацией |
| Нарушители в отношении объектов критической инфраструктуры | Подготовка выступлений на семинарских занятиях с презентациями<br>освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы<br>изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | Выступление на семинарском занятии с презентацией |
| Защита критической информационной инфраструктуры. | Подготовка выступлений на семинарских занятиях с презентациями<br>освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы<br>изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | Выступление на семинарском занятии с презентацией |
| Критические для обеспечения обороны страны, безопасности государства и правопорядка процессы | Подготовка выступлений на семинарских занятиях с презентациями<br>освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы | Игра-симуляция «Атомная электростанция как объект критической инфраструктуры» |

| | | |
|---|---|---|
| | изучение образовательных ресурсов (электронные учебники, электронные библиотеки, электронные видеокурсы и др.) | |

Основная цель самостоятельной работы студента при изучении дисциплины «Защита критической инфраструктуры» – закрепить теоретические знания, полученные в ходе лекционных занятий, сформировать навыки в соответствии с требованиями, определенными в ходе занятий семинарского типа.

Подробная информация о видах самостоятельной работы и оценочных средствах для проверки выполнения самостоятельной работы приведена в Методических рекомендациях по самостоятельной работе обучающихся.

**5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине.**

Образцы заданий текущего контроля и промежуточной аттестации Фонда оценочных средств (ФОС) представлены в Приложении к Рабочей программе дисциплины (модуля) (РПД). В полном объеме ФОС хранится в печатном виде на кафедре, за которой закреплена дисциплина.

**6. Перечень нормативных правовых документов, основной и дополнительной учебной литературы, необходимой для освоения дисциплины «**Защита критической инфраструктуры**».**

**6.1. Нормативные правовые документы**

1. Гражданский кодекс Российской Федерации (часть первая) : федеральный закон от 30.11.1994 N 51-ФЗ : редакция от 27.01.2023.- URL: http://www.consultant.ru/document/cons_doc_LAW_5142/. (дата обращения: 22.01.2025). - Текст: электронный.

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). общероссийского голосования 01.07.2020). - URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 22.01.2025). - Текст : электронный.

3. Трудовой кодекс Российской Федерации : федеральный закон от 30.12.2001 N 197-ФЗ : редакция от 19.12.2022 : с изменениями и дополнениями, вступил в силу с 11.01.2023). - URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 22.01.2025). - Текст : электронный.

4. Федеральный закон «О государственной гражданской службе Российской Федерации» от 27.07.2004 № 79-ФЗ: редакция от14.02.2024. - URL:

http://www.consultant.ru/document/ cons_doc_LAW_48601/ (дата обращения: 22.01.2025). - Текст: электронный.

5. Федеральный закон «Об особенностях прохождения федеральной государственной гражданской службы в системе Министерства иностранных дел Российской Федерации» от 27 июля 2010 г. № 205-ФЗ (последняя редакция). – URL: http://www.consultant.ru/document/cons_doc_LAW_103018/. (дата обращения: 22.01.2025). - Текст: электронный.

**6.2. Основная литература**

1. Белоус, А. И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. - URL: https://biblioclub.ru/index.php?page=book&id=617523 (дата обращения: 09.01.2025). – ISBN 978-5-94836-612-8. – Режим доступа: для авторизир. пользователей. - Текст: электронный.

2. Запечников, С. В. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва: Юрайт, 2024. - 309 с. - ISBN 978-5-534-02574-3. - URL: https://urait.ru/bcode/536453 (дата обращения: 09.01.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. - Москва : Юрайт, 2024. - 325 с. - ISBN 978-5-534-03600-8. - URL: https://urait.ru/bcode/536225 (дата обращения: 09.01.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.

**6.3. Дополнительная литература**

1. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - Москва: РИОР: ИНФРА-М, 2022. - 236 с. - ISBN 978-5-369-01788-3. - URL: https://znanium.ru/catalog/product/1843171 (дата обращения: 04.01.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.

2. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом: учебное пособие для вузов / Е. А. Войниканис; под редакцией М. А. Федотова. - Москва: Юрайт, 2025. - 54 с. - ISBN 978-5-534-21161-0. - URL: https://urait.ru/bcode/559476 (дата обращения: 09.01.2025). – Режим доступа: для авториз. пользователей. – Текст: электронный.

3. Макаренко, С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями: Монография / С. И. Макаренко. - Санкт-Петербург: Наукоемкие технологии, 2018. - 123 с. - ISBN 978-5-6041427-8-3. -

URL: https://book.ru/book/942925 (дата обращения: 09.01.2025). - Режим доступа: для авториз. пользователей. - Текст: электронный.

4. Никитин, А.И. Международные конфликты: вмешательство, миротворчество, урегулирование : учебник / А.И. Никитин. - Москва : Аспект Пресс, 2018. - 384 с. - ISBN 978-5-7567-0928-5. - URL: https://znanium.com/catalog/product/1038562 (дата обращения: 08.01.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.

5. Фисун, В. В., Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры: монография / В. В. Фисун. - Москва: Русайнс, 2020. - 357 с. - ISBN 978-5-4365-6315-2. - URL: https://book.ru/book/939472 (дата обращения: 09.01.2025). – Режим доступа: для авторизир. пользователей. - Текст: электронный.

7. **Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения, профессиональных баз данных и информационных справочных систем**

7.1. Ресурсы информационно-телекоммуникационной сети «Интернет», включая профессиональные базы данных

1. Министерство иностранных дел : официальный сайт. - Москва. - URL: https://mid.ru/. (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.
2. Правительство Российской Федерации : официальный сайт. - Москва. - Обновляется в течение суток. - URL: http://government.ru (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.
3. РАПСИ - Российское агентство правовой и судебной информации. Новости, публикация, законодательство, судебная практика. Мультимедийные материалы. - URL: http://rapsinews.ru/ (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.
4. Ассоциация Деминга : - URL: www//deming.ru/TehnUpr/FunkModOcen.htm. (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.
5. Основы менеджмента: - URL: http://orgmanagement.ru. (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.
6. Центр стратегических исследований : URL: http://www.csr.ru/. (дата обращения: 22.01.2025). - Режим доступа: для авторизир. пользователей. - Текст: электронный.

7.2. Информационно-справочные системы

1. Справочно-правовые системы «Консультант плюс» - www.consultant.ru.
2. Электронная библиотека Дипломатической Академии МИД России на платформе «МегаПро» - https://elib.dipacademy.ru/MegaPro/Web.;

7.3. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства.

Академия обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

-Microsoft Office - 2016 PRO (Полный комплект программ: Access, Excel, PowerPoint, Word и т.д);

-Программное обеспечение электронного ресурса сайта Дипломатической Академии МИД России, включая ЭБС; 1С: Университет ПРОФ (в т.ч., личный кабинет обучающихся и профессорско-преподавательского состава);

-Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версия 3.3 (отечественное ПО);

-Электронная библиотека Дипломатической Академии МИД России на платформе «МегаПро» - https://elib.dipacademy.ru/MegaPro/Web.;

-ЭБС «Лань» - https://e.lanbook.com/.;

-Справочно-информационная полнотекстовая база периодических изданий «East View» - http://dlib.eastview.com.;

-ЭБС «Университетская библиотека - online» - http://biblioclub.ru.;

-ЭБС «Юрайт» - http://www.urait.ru.;

-ЭБС «Book.ru» - https://www.book.ru/.;

-ЭБС «Znanium.com» - http://znanium.com/;

-ЭБС «IPR SMART» - http://www.iprbookshop.ru/.;

-7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО);

-AIMP Бесплатный аудио проигрыватель (лицензия бесплатного программного обеспечения) (отечественное ПО);

-Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения);

-Система видеоконференц связи BigBlueButton (https://bbb.dipacademy.ru) (свободно распространяемое программное обеспечение).

-Система видеоконференц связи «Контур.Талк» (отечественное ПО).

- Система видеоконференц связи МТС.Линк (отечественное ПО).

Каждый обучающийся в течение всего обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе и электронной информационно-образовательной среде.

**8. Описание материально–технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Дисциплина «Защита критической инфраструктуры» обеспечена:

учебной аудиторией для проведения занятий лекционного типа, оборудованной мультимедийными средствами обучения для демонстрации лекций-презентаций, набором демонстрационного оборудования;

учебной аудиторией для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации:420, 424, 385

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде Академии.

**Обновление рабочей программы дисциплины (модуля)**

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Рабочая программа дисциплины: «Защита критической инфраструктуры» обновлена, рассмотрена и одобрена на 20___/___ учебный год на заседании кафедры Стратегических коммуникаций и государственного управления от ____ _____ 20___г., протокол №_____

*Приложение к РПД*

**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Дипломатическая академия Министерства иностранных дел Российской Федерации»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**для проведения текущего контроля, промежуточной аттестации по дисциплине**

**«ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ»**

**направление подготовки:** 38.04.04. государственное и муниципальное управление
**направленность**: гибридные войны: технологии управления и безопасность
**форма обучения:** очная
**квалификация выпускника:** магистр

Москва 2025

**Цель фонда оценочных средств по дисциплине (модулю) «**Защита критической инфраструктуры**»** (далее ФОС) - установление соответствия уровня сформированности компетенций обучающегося, определенных в ФГОС ВО по соответствующему направлению подготовки и ОПОП ВО.

**Задачи ФОС:**

– контроль и управление достижением целей реализации ОПОП, определенных в виде набора компетенций выпускников;

– оценка достижений обучающихся в процессе изучения дисциплины с выделением положительных/отрицательных;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков, определенных в ФГОС ВО и ОПОП ВО;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс Академии.

**Оценочные материалы разрабатываются с учетом следующих принципов:**

-актуальность (соответствие действующим нормативным правовым актам, отраслевым регламентам, ГОСТ (ам) и т.д.);

-адекватность (ориентированность на цели и задачи ОПОП, дисциплины (модуля), практик, НИР, их содержание);

-валидность (возможность использования для «измерения» сформированности компетенций с целью получения объективных результатов);

-точность и однозначность формулировок (недопущение двусмысленного толкования содержания задания);

-достаточность (обеспечение наличия многовариантности заданий);

-наличие разнообразия методов и форм.

## 1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины и предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу данной дисциплины.

Рабочей программой дисциплины «Защита критической инфраструктуры» предусмотрено формирование следующих компетенций: УК-1.1; УК-1.2; УК-6.1; УК-6.2; ПК-5.1; ПК-5.2; ПК-5.3

## 2. Показатели и критерии оценивания контролируемой компетенции на различных этапах формирования, описание шкал оценивания

Применение оценочных средств на этапах формирования компетенций

| Код и наименование формируемой компетенции | Код и формулировка индикатора достижения формируемой компетенции | Результаты обучения | Наименование контролируемых разделов и тем дисциплины (модуля) | Наименование оценочного средства | |
|---|---|---|---|---|---|
| | | | | контрольная точка текущего контроля | промежуточная аттестация |
| **УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | **УК-1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними | **Знает** методику постановки цели и определения способов ее достижения<br>**Умеет** определить суть проблемной ситуации и этапы ее разрешения с учетом вариативных контекстов, осуществлять сбор, систематизацию и критический анализинформации,необходимойдлявыработкистратегиидействийпоразрешению проблемной ситуации | Понятийный аппарат в области защиты критической инфраструктуры (КИ) | **Контрольная работа в виде теста по темам 1-3** | **Вопросы для зачета** |
| | **УК-1.2** Разрабатывает и содежательно аргументирует стратегию решения проблемной ситуации на основе | **Знает** проблемную ситуацию как систему, выявляя ее составляющие и связи между ними<br>**Умеет** проводить оценку адекватности и | Классификация объектов КИ, регламенты обеспечения их безопасности и защиты. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | системного и междисциплинарных подходов | достоверности информации о проблемной ситуации, умеет работать с противоречивой информацией из разных источников**,** осуществлять поиск решений проблемной ситуации на основеействий, эксперимента и опыта, критически оценивать возможные варианты решения пробле-мной ситуации на основе анализа причинно-следственных связей. | | | | |
| **УК-6**. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки | **УК-6.1.**Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их испол-ьзует | **Знает**: основные принципы мотивации и стимулирования карьерного развития, способы самооценки и самоопределения **Умеет:** оценить возможности реализации собственных профессиональных целей и расставить приоритеты | Нарушители в отношении объектов критической инфраструктуры | | | |

| | | | | | |
|---|---|---|---|---|---|
| | **УК-6.2**. Определяет образовательные потребности и способы совершенствования собственной (в том числе профессиональной) деятельности на основе самооценки | **Знает:** особенности деятельностного подхода в исследовании личностного развития.<br>**Умеет**: провести анализ результатов своей социальной и профессиональной деятельности**,** корректировать планы личного и профессионального развития | | | |
| | **ПК-5.1.** Выделяет уровни и виды планирования, организации и проведения информационного сопровождения военных, гуманитарных и иных операций | - Знает основополагающие международно-правовые документы, определяющие порядок информационного сопровождения военных, гуманитарных и иных операций;<br>- Умеет характеризовать значение международно-правовых документов, касающихся применения политических и информационных технологий и противодействия им | Защита критической информационной инфраструктуры. | | |

| | | | | | |
|---|---|---|---|---|---|
| **ПК-5** Способен ориентироваться в особенностях аналитического и информационного сопровождения военных, гуманитарных и иных операций, применения политических и информационных технологий, в том числе стратегических коммуникаций, и противодействия им | **ПК-5.2.** Определяет эффективность организации и проведения информационных кампаний, в том числе стратегических коммуникаций, и противодействия им | - Знает инструменты и механизмы проведения информационных кампаний и противодействия им;<br>- Умеет определять черты различных информационных кампаний и противодействия им; | Понятийный аппарат в области защиты критической инфраструктуры (КИ) | | |
| | **ПК-5.3** Владеет навыками вычленения военных, экономических и политических факторов формирования и реализации современных политических и информационных технологий и противодействия им. | - Знает специфику политизации и технологизации современного информационного поля<br>- Умеет анализировать как целостные стратегии информационного воздействия, так и отдельные продукты и элементы массированных информационных кампаний, а также разрабатывать симметричные и ассиметричные | Классификация объектов КИ, регламенты обеспечения их безопасности и защиты. | | |

| | | | | | |
|---|---|---|---|---|---|
| | | информационные и ментальные антидоты | | | |

**3. Контрольные задания и материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности (индикаторов достижения компетенций), характеризующих результаты обучения в процессе освоения дисциплины (модуля) и методические материалы, определяющие процедуры оценивания**

**3.1. Оценочные средства для проведения текущего контроля**

**Выступления с презентациями**

**Тема 1.** Понятийный аппарат в области защиты критической инфраструктуры

**Тема 2.** Классификация объектов КИ, регламенты обеспечения их безопасности и защиты.

**Тема 3.** Нарушители в отношении объектов критической инфраструктуры.

**Тема 4.** Защита критической информационной инфраструктуры.

| **Выступление на семинарском занятии с презентацией** | |
|---|---|
| 5 баллов | Подготовил полное и развернутое выступление;<br>Активно обсуждал проблему и обосновывал свою позицию;<br>Использовал терминологию, концепции, теории при решении проблем административной деятельности;<br>Проявил высокий уровень способности объективно оценивать проблемы административной деятельности, учитывать их в сфере профессиональной деятельности;<br>Презентацию подготовил в едином стиле, на базе одного шаблона<br>Выполнил общие правила оформления текста;<br>Не перегрузил слайды текстовой информацией. |
| 3-4 балла | Подготовил не полное выступление;<br>Слабо принимал участие в обсуждении проблемы;<br>Редко использовал терминологию, концепции, теории при решении проблем административной деятельности;<br>Проявил низкую способность объективно оценивать проблемы административной деятельности, учитывать их в сфере профессиональной деятельности;<br>Перегрузил презентацию слайдами текстовой информацией; |
| 0-2 балла | Подготовил не полное выступление<br>Не подготовил презентацию. |

**Тема 5.**
Игра-симуляция «Атомная электростанция как объект критической инфраструктуры». Подробнее о подготовке и ходе игры см. в Методических указаниях по подготовке к игре-симуляции «Атомная электростанция как объект критической инфраструктуры».

На примере Запорожской АЭС (одна подгруппа) и Фукусимской АЭС (вторая подгруппа) происходит моделирование заседания штаба по ЧС. Задача штаба – определить уязвимости, риски, угрозы, разработать систему мер по обеспечению безопасности объекта КИ. Эксперты МАГАТЭ (третья подгруппа) оценивают план мероприятий. Цель симуляции – усовершенствование плана мероприятий по нейтрализации рисков и угроз, попыток атак на объект КИ.

**Критерии оценивания участия в игре-симуляции**

| | |
|---|---|
| Макс. 9-10 баллов (*в соответствии с балльно-рейтинговой системой )* | Активное участие в дискуссии (более 10 реплик), с опорой на теорию МО, с элементами анализа |
| 6-8 баллов | Участие в дискуссии по основным вопросам обсуждения (5-9 реплик), с опорой на теорию МО, без элементов анализа |
| 3-5 баллов | Участие в дискуссии только по запросу модератора (3-4 реплики), с опорой на теорию МО, без элементов анализа |
| 0-2 балла | Отсутствие реплик/несодержательные реплики, без опоры на теорию МО, без элементов анализа |

Текущий контроль по дисциплине проводится 1 раза за период освоения дисциплины. В качестве контрольной точки для проведения текущего контроля успеваемости по дисциплине используется: контрольная работа в виде теста

**Контрольная работа в виде теста**

1. **Гражданин РФ У., замещая должность помощника депутата Государственной Думы РФ и имея соответствующую форму допуска к информации, являющейся секретной, посетил вместе с депутатом полигон, на котором производились испытания принципиально новых моделей тяжелого стрелкового оружия. Через три дня после возвращения с полигона гражданин У., находясь в ресторане с друзьями, познакомился с гражданином иностранного государства В. В общей беседе гражданин У. рассказал присутствующим (в т.ч. и В) о своей поездке и описал процедуру испытаний, а также возможности испытанных образцов. Через два дня после этого гражданина У. вызвали повесткой в территориальное управление ФСБ РФ, где в ходе беседы со следователем по особо важным делам гражданином РФ П. (специальное звание майор) гражданину У. было предъявлено обвинение в шпионаже в пользу иностранного государства, гражданином которого был В., на тот момент уже задержанный также по обвинению в шпионаже и дающий соответствующие показания. Верное ли было предъявлено обвинение гражданину У.?**

А. нет, неверное, поскольку гражданин У. передал секретные сведения, ставшие

ему известными в связи с выполнением должностных обязанностей, не собирая их специально

B. нет, неверное, поскольку в отношении гражданина иностранного государства В. отсутствует приговор суда, указывающий на вынесение наказания по факту деяния в форме шпионажа

C. да, верное, поскольку гражданин У. передал секретные сведения лицу, изобличенному в шпионаже собственными показаниями такого лица

D. да, верное, поскольку гражданин У. собирал сведения, находясь на полигоне, с целью их передачи в процессе беседы

**2. Чему должна соответствовать степень секретности сведений, составляющих государственную тайну?**

A. степени власти лиц, допущенных к таким сведениям

B. степени тяжести ущерба, который может быть нанесен безопасности государства вследствие распространения указанных сведений

C. степени сложности собирания, добычи, получения иным способом таких сведений

D. степени редкости таких сведений

**3. Соотнесите наименования типов и видов сведений, составляющих государственную тайну.**

**1.** сведения в военной области

**2.** сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

**3.** сведения в области внешней политики и экономики

**4.** сведения в области экономики, науки и техники

A. сведения об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства

B. сведения о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации

C. сведения о финансовой политике в отношении иностранных государств

D. сведения о режимных и особо важных объектах

**4. Что из перечисленного относят к критической инфраструктуре?**

A. Министерство внутренних дел
B. Кремль
C. ФСБ
D. Электростанции, плотины, системы водоснабжения, мосты и т.д.

**5. В той или иной степени все сектора критической инфраструктуры зависят от информационных технологий.**

A. Ложь
B. Верно

**6. Инфраструктура относится к базовой структуре, которая позволяет обществу функционировать.**

A. Верно
B. Ложь

**7. Какой нормативный документ устанавливает требования к созданию систем безопасности КИИ РФ?**

1. ФЗ от 27 июля 2017 г. №187 ФЗ
2. Приказ ФСТЭК России от 21 декабря 2017 г. № 135
3. Постановление Правительства РФ от 22 декабря 2023 г. № 3142
4. В российском законодательстве нет таких требований.

**8. В качестве исходных данных для анализа угроз информации используются:**

A. Сведения об уязвимости безопасности информации
B. Сведения об угрозах безопасности информации
C. Банк данных угроз безопасности ФСТЭК
D. Показания пользователя системы

**9. Что осуществляется при проектировании подсистемы безопасности значимого объекта?**

A. Проводится технико-экономическое обоснование затрат на защиту
B. Определяются виды и типы средств защиты
C. Осуществляется выбор средств защиты
D. Проводится оценка угроз и уязвимости системы

**10. Каковы обязанности субъекта КИИ?**

A. Информировать о компьютерных инцидентах уполномоченный федеральный орган исполнительной власти
B. Оказывать содействие уполномоченному федеральному органу исполнительной власти в обнаружении, предупреждении и ликвидации последствий компьютерных атак
C. Обеспечивать выполнение порядка, технических условий установки и эксплуатации средств защиты от компьютерных атак
D. Передавать данные третьим лицам

| | |
|---|---|
| *Макс. 9-10 баллов (в соответствии с балльно-рейтинговой системой )* | *10 правильных ответов (100 % ответов)* |
| *6-8 баллов* | *7-9 правильных ответов (67-80 % ответов)* |
| *3-5 баллов* | *3-6 правильных ответов (50-66 % ответов)* |
| *0-2 балла* | *0-2 правильных ответов (менее 50% ответов)* |

### 3.2. Оценочные средства для проведения промежуточной аттестации

В качестве оценочного средства для проведения промежуточной аттестации по дисциплине используется: *зачет*

| № п/п | Форма контроля | Наименование оценочного средства | Представление оценочного средства в фонде |
|---|---|---|---|
| 1. | зачет | Зачет в устной форме, в билете по 1 вопросу | Перечень вопросов |

### Перечень вопросов к зачету

1. Субъект и объект критической инфраструктуры,
2. Автоматизированная система управления,
3. Понятие безопасности КИ,
4. Государственная тайна: понятие, уровни доступа, меры по сохранению, ответственность за нарушение. Гриф секретности
5. Понятие государственной информационной системы.
6. Доступ к информации, доступность информации,
7. Информационно-телекоммуникационная сеть,
8. Понятие инцидента информационной безопасности. Компьютерный инцидент
9. Компьютерная атака: понятие, классификация, механизмы защиты.
10. Понятие критической информационной инфраструктуры (КИИ), конфиденциальность информации и т.д.)

11. Классификация объектов КИ, регламенты обеспечения их безопасности и защиты.
12. Энергетика и коммунальные услуги как объекты КИ: поставщики электроэнергии; нефть и газ; поставки угля, природного газа; мазут для дома; поставки для АЗС; поставщики альтернативной энергии (ветровой, солнечной, другой).
13. Информационно-коммуникационные технологии как объекты КИ: средства вещания; телекоммуникационные провайдеры (стационарные, сотовые телефоны, интернет, Wi-Fi)
14. Почтовые услуги как объекты КИ
15. Финансы как объекты КИ: банковские услуги, государственные департаменты финансов / помощи; налогообложение.
16. Здоровье как объекты КИ: Программы общественного здравоохранения и оздоровления, помещения больниц / клиник; кровь и продукты крови
17. Продукты питания как объекты КИ: цепочки поставок продуктов питания; продовольственные инспекторы; программы импорта / экспорта; продуктовые магазины
18. Сельскохозяйственная культура как объект КИ; фермерские рынки.
19. Вода как объекты КИ: Водоснабжение и охрана; управление сточными водами; программы рыболовства и защиты океана.
20. Транспорт как объекты КИ: дороги, мосты, железные дороги, авиация / аэропорты; судоходство и порты; транзит.
21. Службы экстренного реагирования как объекты КИ.
22. Основные сектора КИ.
23. Нарушители в отношении объектов критической инфраструктуры (классификация по оснащенности, знаниям, мотивации).
24. Защита критической информационной инфраструктуры.
25. Методики определения угроз безопасности информации в информационных системах.
26. Критические для обеспечения обороны страны, безопасности государства и правопорядка процессы: управленческие, технологические, производственные, финансово-экономические.
27. Механизмы корректировки критических процессов, их нейтрализации и перезапуска.
28. Технология стресс-тестирования: предварительная оценка контекста риска и контекста опасности, собственно стресс-тест, принятие решения по стратегии снижения рисков, отчет с рекомендациями по снижению рисков).

**Критерии оценивания(зачет)**

**30-60 баллов** ставится в том случае, когда обучающийся обнаруживает систематическое и глубокое знание программного материала по дисциплине, умеет свободно ориентироваться в вопросе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Обучающийся уверенно отвечает на дополнительные вопросы.

**менее 30 баллов** ставится в том случае, когда обучающийся не обнаруживает знание основного программного материала по дисциплине, допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены неправильно, обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

Итоговый результат аттестационных испытаний по дисциплине за семестр выставляется в соответствии с Положением о балльно-рейтинговой системе, утвержденным приказом ректора Академии №11-05-45 от 03 марта 2023 г.

Результатом освоения дисциплины «Защита критической инфраструктуры» является установление одного из уровней сформированности компетенций: высокий (продвинутый), хороший, базовый, недостаточный.

Показатели уровней сформированности компетенций

| **Уровень/балл** | **Универсальные компетенции** | **Профессиональные компетенции** |
|---|---|---|
| Высокий (продвинутый) (оценка «отлично», «зачтено») **86-100** | *Сформированы четкие системные знания и представления по дисциплине.* *Ответы на вопросы оценочных средств полные и верные.* *Даны развернутые ответы на дополнительные вопросы.* *Обучающимся продемонстрирован высокий уровень освоения компетенции* | *Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач.* *Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы.* *Обучающимся продемонстрирован высокий уровень освоения компетенции* |
| Хороший (оценка «хорошо», «зачтено») **71-85** | *Знания и представления по дисциплине сформированы на повышенном уровне.* *В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия.* *Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки.* *Обучающимся продемонстрирован повышенный уровень освоения компетенции* | *Сформированы в целом системные знания и представления по дисциплине.* *Ответы на вопросы оценочных средств полные, грамотные.* *Продемонстрирован повышенный уровень владения практическими умениями и навыками.* *Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков* |
| Базовый (оценка «удовлетворительно», «зачтено») **56-70** | *Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП.* *Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения.* *Обучающимся продемонстрирован базовый уровень освоения компетенции* | *Обучающийся владеет знаниями основного материал на базовом уровне.* *Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач* |

| Уровень/балл | Универсальные компетенции | Профессиональные компетенции |
|---|---|---|
| Недостаточный (оценка «неудовлетворительно», «не зачтено») **Менее 56** | *Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков* | *Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков* |

*Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.*

**Обновление фонда оценочных средств**

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Фонд оценочных средств в составе Рабочей программы дисциплины: «Защита критической инфраструктуры» обновлен, рассмотрен и одобрен на 20___/___ учебный год на заседании кафедры Государственного управления во внешнеполитической деятельности от ____ _____ 20___г., протокол №_____