МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Реагирование на инциденты информационной безопасности объектов критической информационной инфраструктуры

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану	216	Виды контроля в семестрах:
в том числе:		зачеты 11
аудиторные занятия	112,25	
самостоятельная работа	103,75	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**11 (6.1)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	56	56	56	56
Лабораторные	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	8	8	8	8
Итого ауд.	112,25	112,25	112,25	112,25
Контактная работа	112,25	112,25	112,25	112,25
Сам. работа	103,75	103,75	103,75	103,75
Итого	216	216	216	216

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель: освоение студентами технологий реагирования на инциденты информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ).
1.2	Задачи: освоение теоретических основ реагирования на инциденты ИБ;
1.3	освоение нормативных основ реагирования на инциденты ИБ объектов КИИ;
1.4	освоение технологий обнаружения, расследования и устранения инцидентов ИБ на объектах КИИ.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.10
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-6: Способен обнаруживать, идентифицировать и устранять инциденты, возникшие в процессе эксплуатации автоматизированных систем	
Знать:	
Уровень 1	Условия и ограничения успешного выполнения порученной работы на основе собственных личностных, ситуативных, профессиональных качеств и возможности их совершенствования
Уровень 2	Основы эффективного использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата;
Уровень 3	инструменты и методы управления временем при выполнении конкретных задач, выстраивания траектории собственного профессионального роста
Уметь:	
Уровень 1	Применять знания о своих ресурсах и их пределах (личностных, ситуативных, временных и т.д.), для успешного выполнения порученной работы;
Уровень 2	Определять приоритеты собственной деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда;
Уровень 3	Проводить оценку современных требований рынка труда для выстраивания траектории собственного профессионального развития
Владеть:	
Уровень 1	информацией о потребностях рынка труда в образовательных услугах для выстраивания траектории собственного профессионального развития
Уровень 2	навыками реализации намеченных целей деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда
Уровень 3	Способами оценки эффективности использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	порядок проведения расследования компьютерных инцидентов на значимых объектах критической информационной инфраструктуры
3.2	**Уметь:**
3.2.1	осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;
3.2.2	определять источники и причины возникновения компьютерных инцидентов
3.3	**Владеть:**
3.3.1	проведения расследования инцидентов на средствах вычислительной техники и телекоммуникационном оборудовании значимых объектов критической информационной инфраструктуры

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Введение. Базовые понятия курса.						
1.1	Введение. Базовые понятия курса. /Лек/	11	8		Л1.1	0	

1.2	Введение. Базовые понятия курса. /Пр/	11	4		Л1.1	0	
	Раздел 2. Организационно-правовые основы реагирования на инциденты ИБ на объектах КИИ						
2.1	Организационно-правовые основы реагирования на инциденты ИБ на объектах КИИ /Лек/	11	8		Л1.1	0	
2.2	Правовые и организационные основы реагирования на инциденты ИБ на объектах КИИ /Пр/	11	4		Л1.1	4	
	Раздел 3. Этапы реагирования на инциденты ИБ объектов КИИ						
3.1	Этапы реагирования на инциденты ИБ на объектах КИИ /Лек/	11	10		Л1.1	0	
3.2	Этапы реагирования на инциденты ИБ на объектах КИИ /Пр/	11	6		Л1.1	0	
	Раздел 4. Методики производства компьютерной экспертизы						
4.1	Методики производства компьютерной экспертизы /Лек/	11	10		Л1.1	0	
	Раздел 5. Инструментальные средства расследования инцидентов ИБ объектов КИИ						
5.1	Инструментальные средства расследования инцидентов ИБ объектов КИИ /Лек/	11	10		Л1.1	0	
5.2	Инструментальные средства реагирования на инциденты ИБ на объектах КИИ /Пр/	11	8		Л1.1	0	
5.3	Моделирование технологий реагирования /Ср/	11	103,75		Л1.1	0	
	Раздел 6. Документационное сопровождение расследования инцидентов ИБ объектов КИИ						
6.1	Документационное сопровождение расследования инцидентов ИБ на объектах КИИ /Лек/	11	10		Л1.1	0	
6.2	Документационное сопровождение реагирования на инциденты ИБ на объектах КИИ /Пр/	11	6		Л1.1	0	
6.3	Зачет /ИВКР/	11	0,25		Л1.1	0	
6.4	Документационное сопровождение расследования инцидентов ИБ на объектах КИИ /Лаб/	11	28		Л1.1	4	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Введение. Базовые понятия курса

1. Что такое критическая информационная инфраструктура (КИИ)? Приведите примеры объектов КИИ.
2. Какие ключевые принципы обеспечения информационной безопасности на объектах КИИ?
3. Что такое инцидент информационной безопасности? Как классифицируются инциденты (например, по уровню угрозы, типу атаки)?
4. Какие цели и задачи курса по реагированию на инциденты ИБ на объектах КИИ?
5. Какие международные и отечественные стандарты регулируют защиту КИИ (например, ГОСТ Р 57580, ISO/IEC 27014, NIST SP 800-61)?

Тема: 2. Организационно-правовые основы реагирования

6. Какие нормативные правовые акты регулируют реагирование на инциденты ИБ на объектах КИИ в РФ (ФЗ-187, ФЗ-149, указы Президента)?
7. Какие функции выполняет Центр реагирования на компьютерные инциденты (ЦРКИ) при работе с КИИ?
8. Как организуется взаимодействие между службами безопасности, правоохранительными органами и регуляторами (например, ФСТЭК, ФСБ) при инцидентах на КИИ?
9. Что такое план реагирования на инциденты ИБ? Какие разделы обязательны для объектов КИИ?

10. Какие требования к обучению персонала и тестированию готовности к инцидентам установлены для объектов КИИ?
Тема: 3. Этапы реагирования на инциденты ИБ
11. Какие этапы жизненного цикла реагирования на инциденты ИБ выделяются (подготовка, обнаружение, анализ, локализация, устранение, восстановление, постинцидентный анализ)?
12. Как организуется мониторинг инцидентов в режиме реального времени на объектах КИИ?
13. Какие критерии используются для классификации инцидентов (например, уровень угрозы, влияние на бизнес-процессы)?
14. Как проводится локализация инцидента в распределенных системах КИИ (например, АСУ ТП, энергетические сети)?
15. Какие меры восстановления применяются после устранения инцидента? Как обеспечивается целостность данных и систем?
Тема: 4. Методики компьютерной экспертизы
16. Какие этапы включает процесс компьютерной экспертизы при расследовании инцидентов ИБ?
17. Какие требования к сбору и сохранению цифровых доказательств на объектах КИИ?
18. Как используются методики DFIR (Digital Forensics and Incident Response) для анализа атак?
19. Какие инструменты и подходы применяются для восстановления событий (лог-анализ, memory dump, анализ трафика)?
20. Как обеспечивается юридическая значимость результатов компьютерной экспертизы (например, соблюдение ФЗ-162)?
Тема: 5. Инструментальные средства расследования инцидентов
21. Какие программные средства используются для обнаружения инцидентов (SIEM, EDR, IDS/IPS)?
22. Как работают системы анализа логов (например, Splunk, QRadar) в контексте КИИ?
23. Какие инструменты применяются для анализа памяти и дампов сетевого трафика (например, Volatility, Wireshark)?
24. Как используются платформы для автоматизации расследований (SOAR, например, Siemplify, IBM Resilient)?
25. Какие специализированные инструменты применяются для анализа вредоносного ПО (например, Cuckoo Sandbox, ANY.RUN)?
Тема: 6. Документационное сопровождение расследований
26. Какие документы обязательны при регистрации и расследовании инцидентов ИБ (например, журнал инцидентов, акт расследования)?
27. Как оформляется отчет по результатам инцидента (структура, содержание)?
28. Какие требования к хранению и передаче информации о инциденте (например, ограничения по доступу, шифрование)?
29. Как документируется процесс компьютерной экспертизы для обеспечения юридической значимости?
30. Какие метрики и KPI используются для оценки эффективности реагирования (например, MTTD, MTTR)?
Тема: 7. Специфика объектов КИИ
31. Какие особенности реагирования на инциденты в АСУ ТП по сравнению с корпоративными сетями?
32. Какие риски возникают при атаках на инфраструктуру жизнеобеспечения (энергетика, транспорт)?
33. Какие меры предпринимаются для минимизации воздействия инцидентов на непрерывность технологических процессов?
34. Как организуется резервное копирование и аварийное восстановление на объектах КИИ?
35. Какие сценарии атак наиболее актуальны для КИИ (например, ransomware, APT, DDoS)?
Тема: 8. Современные вызовы и угрозы
36. Какие угрозы связаны с интеграцией IoT и OT-устройств в системы КИИ?
37. Как искусственный интеллект и машинное обучение используются для обнаружения инцидентов?
38. Какие проблемы возникают при защите гибридных систем (локальные + облачные)?
39. Как квантовые технологии могут повлиять на безопасность объектов КИИ в будущем?
40. Какие угрозы связаны с утечкой данных через побочные каналы (TEMPEST, акустический шум)?
Тема: 9. Практические аспекты
41. Как провести симуляцию атаки (red team/blue team) на объекте КИИ?
42. Какие этапы включает пентестинг критических систем? Как обеспечить безопасность при тестировании?
43. Как организовать расследование инцидента с использованием MITRE ATT&CK для КИИ?
44. Какие кейсы инцидентов на объектах КИИ известны (например, атака на украинскую энергосеть, Stuxnet)?
45. Как подготовить организацию к аудиту соответствия требованиям защиты КИИ (например, по ФЗ-187)?
Тема: 10. Международный опыт и стандарты
46. Какие отличия в подходах к защите КИИ в ЕС (NIS, NIS2), США (NIST, CISA) и России?
47. Какие стандарты и фреймворки используются для управления инцидентами (например, ISO/IEC 27035, NIST IR)?
48. Как организованы CSIRT-команды в других странах? Какие функции они выполняют?
49. Как международное сотрудничество (например, INTERPOL, ENISA) помогает в борьбе с киберугрозами на КИИ?
50. Какие уроки из зарубежных инцидентов (например, Colonial Pipeline, SolarWinds) применимы к российским объектам КИИ?

5.2. Темы письменных работ

Не предусмотрены

5.3. Оценочные средства

Рабочая программа "Реагирование на инциденты информационной безопасности объектов критической информационной инфраструктуры" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: зачета в 11 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Вехов В. Б., Зуев С. В., Бахтеев Д. В., Буглаева Е. А., Ковалев С. А., Никитин Е. В., Русман Г. С., Смахтин Е. В., Христинина Е. В.	Цифровая криминалистика: учебник для вузов	Москва: Юрайт, 2024

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	
6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.

6.3.2 Перечень информационных справочных систем

6.3.2.1	База данных научных электронных журналов "eLibrary"
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	Лаб

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Реагирование на инциденты информационной безопасности объектов критической информационной инфраструктуры" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.