МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Технологии защиты информации в различных отраслях деятельности

рабочая программа дисциплины (модуля)

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

Учебный план b090302_25_BIS25.plx
09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 0
в том числе:
аудиторные занятия 0
самостоятельная работа 0

Виды контроля в семестрах:

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	0,25	0,25	0,25	0,25
Итого ауд.	56,25	56,25	56,25	56,25
Контактная работа	56,25	56,25	56,25	56,25
Сам. работа	87,75	87,75	87,75	87,75
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины:
1.2	– изучение комплекса мер, операций и приемов, направленных на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на защищаемую информацию в следующих сферах
1.3	-деятельности в сфере федерального и регионального управления и электронной коммерции.
1.4	Основная задача дисциплины:
1.5	– вооружить студентов теоретическими знаниями и практическими навыками, необходимыми для быстрой адаптации и успешной профессиональной деятельности в части защиты информации в различных отраслях деятельности;
1.6	- обеспечения устойчивости функционирования информационных объектов в различных отраслях деятельности;
1.7	-выработке и принятию организационно-технических решений адекватных степени угроз;
1.8	-реализации эффективных мер по защите информационных систем на этапах их проектирования и внедрения и эксплуатацию.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Инженерно-техническая защита информации и технические средства охраны
2.1.2	Практикум по решению проектных задач профессиональной деятельности
2.1.3	Основы аттестации объектов информатизации
2.1.4	Методы и средства противодействия террористической деятельности в системах управления значимых объектов КИИ
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-6.3: Способен выполнять работы по выявлению и устранению инцидентов в информационно-коммуникационных системах
Знать:
Уметь:
Владеть:

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	цели и задачи проектирования систем инженерно-технической защиты объектов;
3.1.2	основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов;
3.1.3	основные принципы проектирования систем инженерно-технической защиты объектов, физические принципы, на которых строятся системы инженерно-технической защиты объектов
3.2	**Уметь:**
3.2.1	проводить анализ вероятных угроз охраняемому объекту;
3.2.2	выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту;
3.2.3	выбирать технические средства для решения задачи охраны объекта, проводить оптимизацию структуры комплексов инженерно-технической защиты объектов
3.3	**Владеть:**
3.3.1	анализа критериев оценки параметров технических средств охраны объектов;
3.3.2	составления программы испытаний систем инженерно-технической защиты объектов

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. Технологии защиты информации в электронной коммерции						

1.1	Понятие электронной коммерции. Электронная торговля. Электронное движение капитала.Электронный маркетинг. Электронные страховые услуги /Лек/	8	4		Л1.1	0	
1.2	Криптовалюты и блокчейн в электронной коммерции /Лек/	8	4		Л1.1	0	
1.3	Защита персональных данных в электронной коммерции /Лек/	8	4		Л1.1	0	
1.4	Понятие электронной коммерции. Основные уязвимости информационных систем, применяемых в электронной коммерции /Пр/	8	2		Л1.1	0	
1.5	Моделирование системы средств и методов защиты информации в электронной коммерции /Пр/	8	2		Л1.1	0	
1.6	Деловая игра: комплексное обеспечение информационной безопасности интернет-магазина /Пр/	8	2		Л1.1	0	
1.7	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 1) /Ср/	8	29		Л1.1	0	
	Раздел 2. Технологии защиты информации в кредитно-финансовой сфере						
2.1	Понятие платежных систем. Интернет-банкинг. Электронный обмен данными (EDI) /Лек/	8	4		Л1.1	0	
2.2	Методы и средства защиты информации в кредитно-финансовой сфере /Лек/	8	4		Л1.1	0	
2.3	Защита банковской тайны, структура информационных потоков, Понятие платежных систем. Интернет-банкинг. Электронный обмен данными (EDI) /Пр/	8	2		Л1.1	0	
2.4	Защита информации в банковской сфере: криптография, блокчейн и криптовалюты /Пр/	8	4		Л1.1	0	
2.5	Разработка схемы бизнес-процессов для предприятий, работающих с EDI /Пр/	8	4		Л1.1	0	
2.6	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 2) /Ср/	8	29		Л1.1	0	
	Раздел 3. Технологии защиты информации в органах государственной власти и муниципального управления						
3.1	Информационная безопасность в ГИС , законодательство, этапы проектирования информационной среды /Лек/	8	2		Л1.1	0	

3.2	Электронная подпись и инфраструктура открытых ключей: лицензирование и аккредитация /Лек/	8	2		Л1.1	0	
3.3	Методы и средства защиты информации в органах государственной власти и муниципального управления /Лек/	8	4		Л1.1	0	
3.4	Виды информации ограниченного доступа, обрабатываемых в автоматизированных системах органов государственной власти и муниципального управления /Пр/	8	4		Л1.1	0	
3.5	Информационная безопасность в ГИС , законодательство, этапы проектирования информационной среды. Электронная подпись и инфраструктура открытых ключей: лицензирование и аккредитация /Пр/	8	4		Л1.1	0	
3.6	Защита информации в ГИС, ЗОКИИ и ИСПДН органов государственной власти и муниципального управления. /Пр/	8	4		Л1.1	0	
3.7	Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (раздел 3) /Ср/	8	29,75		Л1.1	0	
3.8	Зачет /ИВКР/	8	0,25		Л1.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Основы электронной коммерции
1. Каково определение электронной коммерции? Какие ключевые компоненты входят в её состав?
2. Чем отличаются электронная торговля, электронное движение капитала и электронный маркетинг? Приведите примеры.
3. Какие виды электронной коммерции выделяют (B2B, B2C, C2C, G2B)? Охарактеризуйте каждый.
4. Какие особенности электронных страховых услуг? Какие риски связаны с их цифровизацией?
5. Как электронная коммерция влияет на традиционные бизнес-модели?
Тема: 2. Криптовалюты и блокчейн
6. Что такое блокчейн? Какие основные принципы его работы?
7. Как криптовалюты (например, Bitcoin, Ethereum) используются в электронной коммерции?
8. Какие преимущества и риски использования блокчейн-технологий в бизнесе?
9. Какие регуляторные вызовы связаны с криптовалютами (например, AML, KYC)?
10. Приведите примеры применения блокчейна за пределами финансовых услуг.
Тема: 3. Защита персональных данных
11. Какие основные принципы защиты персональных данных в электронной коммерции?
12. Как регулируется защита данных в ЕС (GDPR) и России (ФЗ-152)? Чем они отличаются?
13. Какие методы шифрования и анонимизации данных применяются для защиты персональных данных?
14. Какие угрозы связаны с утечкой данных в электронной коммерции? Приведите примеры.
15. Как обучение сотрудников влияет на уровень безопасности персональных данных?
Тема: 4. Платежные системы и интернет-банкинг
16. Что такое платежная система? Какие виды платежных систем существуют (например, банковские, мобильные, криптовалютные)?
17. Как устроена система интернет-банкинга? Какие меры безопасности реализованы в онлайн-банках?
18. Что такое EDI (электронный обмен данными)? Как он используется в логистике и торговле?
19. Какие риски связаны с цифровыми платежами (например, мошенничество, двойные транзакции)?
20. Как регулируются платежные системы в России (например, ЦБ РФ) и за рубежом?
Тема: 5. Методы и средства защиты информации в финансовой сфере
21. Какие технологии шифрования применяются в кредитно-финансовой сфере (например, TLS, RSA)?
22. Что такое двухфакторная аутентификация? Как она реализуется в онлайн-банкинге?
23. Какие системы обнаружения мошенничества используются в банках (например, ML, биометрия)?
24. Какие угрозы наиболее актуальны для финансовых организаций (например, DDoS, фишинг)?

25. Как регулярное тестирование на проникновение (пентестинг) помогает улучшить безопасность?
Тема: 6. Информационная безопасность в ГИС
26. Какие особенности защиты данных в геоинформационных системах (ГИС)?
27. Какие законы регулируют использование геоданных в России (например, ФЗ-149)?
28. Какие этапы проектирования безопасной информационной среды в ГИС?
29. Как анонимизация и псевдонимизация данных используются в ГИС?
30. Какие угрозы связаны с использованием ГИС в государственных и частных секторах?
Тема: 7. Электронная подпись и инфраструктура открытых ключей
31. Какие виды электронной подписи регулируются законодательством (простая, усиленная, квалифицированная)?
32. Что такое инфраструктура открытых ключей (PKI)? Какие компоненты в неё входят?
33. Как проходит процесс лицензирования и аккредитации удостоверяющих центров?
34. Как электронная подпись используется в государственных и корпоративных системах?
35. Какие альтернативы электронной подписи существуют (например, блокчейн-подписи)?
Тема: 8. Безопасность в органах муниципального управления
36. Какие угрозы информационной безопасности актуальны для органов власти?
37. Какие нормативные документы регулируют ИБ в государственных и муниципальных организациях?
38. Какие меры защиты информации реализуются в электронном правительстве (e-Gov)?
39. Как обучение персонала влияет на уровень безопасности в муниципальных системах?
40. Какие примеры успешного внедрения мер ИБ в муниципальных проектах?
Тема: 9. Современные вызовы и тенденции
41. Как искусственный интеллект и машинное обучение используются для обеспечения ИБ в электронной коммерции?
42. Как облачные технологии влияют на безопасность данных в финансовой сфере?
43. Как квантовые вычисления могут повлиять на будущее криптографии?
44. Как защитить данные от утечки через побочные электромагнитные излучения (TEMPEST)?
45. Как использовать блокчейн для защиты целостности данных в государственных системах?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Технологии защиты информации в различных отраслях деятельности" 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	Советов Б. Я., Цехановский В. В., Чертовской В. Д.	Базы данных: 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	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"
6.3.2.3	База данных научных электронных журналов "eLibrary"

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	

		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 "Технологии защиты информации в различных отраслях деятельности" 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.