МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Криптографические протоколы

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 64,25
самостоятельная работа 43,75

Виды контроля в семестрах:
зачеты 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	43,75	43,75	43,75	43,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является изучение студентами основных видов современных криптографических протоколов, методов их анализа и оценки стойкости, основных сфер практического применения и особенностей реализации.
1.2	Задачами дисциплины являются:
1.3	- ознакомление студентов со структурой современных сложных криптосистем, основными классами криптографических протоколов;
1.4	- обзор методов анализа стойкости криптографических протоколов и средств криптографической защиты информации, в которых они реализуются;
1.5	- изучение основных нормативно-технических документов, регламентирующих применение криптографических методов защиты информации, а также проектирование, разработку и применение средств криптографической защиты информации.

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	
Знать:	
Уровень 1	основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы;
Уровень 2	национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; предназначение криптографических протоколов в реализации политик информационной безопасности;
Уровень 3	область применения криптографических протоколов в системе защиты автоматизированных систем;
Уметь:	
Уровень 1	использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности;
Уровень 2	производить вычисления в алгебраических структурах (группах, кольцах и полях); применять теоретико-графовые и теоретико-множественные методы при реализации протоколов;
Уровень 3	производить аудит результатов выполненного протокола;
Владеть:	
Уровень 1	криптографической терминологией;
Уровень 2	навыками применения криптографических протоколов при решении задач профессиональной деятельности;
Уровень 3	навыками применять изучаемый математический аппарат для исследования свойств криптографических преобразований;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	основные понятия и задачи криптографии, математические модели криптографических систем;
3.1.2	основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш- функции и криптографические протоколы;
3.1.3	национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения
3.2	**Уметь:**
3.2.1	использовать систему криптографической защиты информации (СКЗИ) для решения задач профессиональной деятельности
3.3	**Владеть:**

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. Основные понятия						
1.1	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов. /Лек/	7	6	ОПК-10	Л1.1 Л1.2	0	
1.2	Примеры протоколов на основе симметричных и асимметричных криптографических систем. /Пр/	7	6	ОПК-10	Л1.1 Л1.2	1	
	Раздел 2. Схемы цифровой подписи						
2.1	Схемы цифровой подписи. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Стандарты США и России электронной цифровой подписи. Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки. /Лек/	7	6	ОПК-10	Л1.1 Л1.2	0	
2.2	Примеры схем цифровых подписей. Контрольная работа "Цифровые подписи" /Пр/	7	6	ОПК-10	Л1.1 Л1.2	1	
	Раздел 3. Протоколы идентификации						
3.1	Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. /Лек/	7	2	ОПК-10	Л1.1 Л1.2	0	
3.2	Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением /Лек/	7	6	ОПК-10	Л1.1 Л1.2	0	
3.3	Протоколы «рукопожатия» и идентификации типа «запрос-ответ» с криптографической терминологией Протоколы доказательства знания с нулевым разглашением /Пр/	7	6	ОПК-10	Л1.1 Л1.2	1	
3.4	Контрольная работа "Игровые протоколы" /Пр/	7	6	ОПК-10	Л1.1 Л1.2	1	
3.5	Разработка программ, реализующих различные криптографические протоколы. /Ср/	7	33,75	ОПК-10	Л1.1 Л1.2	0	
	Раздел 4. Протоколы открытых сделок						

4.1	Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. /Лек/	7	4	ОПК-10	Л1.1 Л1.2	0	
4.2	Протоколы электронного голосования. Протокол использования электронных денег /Лек/	7	2	ОПК-10	Л1.1 Л1.2	0	
4.3	Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.) /Пр/	7	8	ОПК-10	Л1.1 Л1.2	0	
	Раздел 5. Прикладные протоколы						
5.1	Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. /Лек/	7	2	ОПК-10	Л1.1 Л1.2	0	
5.2	Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. /Лек/	7	2	ОПК-10	Л1.1 Л1.2	0	
	Раздел 6. Нормативные документы в области криптографических протоколов.						
6.1	Протоколы SKIP, SSL/TLS и особенности их реализации. /Лек/	7	2	ОПК-10	Л1.1 Л1.2	0	
6.2	Подготовка к практическим занятиям, выполнение домашних заданий. /Ср/	7	10	ОПК-10	Л1.1 Л1.2	0	
6.3	Зачет /ИВКР/	7	0,25	ОПК-10	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Основы криптографических протоколов
1. Что такое криптографический протокол и какова его роль в защите информации?
2. Какие основные свойства обеспечивают безопасность криптографических протоколов?
3. Какие виды уязвимостей характерны для криптографических протоколов?
4. Как классифицируются криптографические протоколы?
5. Какие подходы используются для моделирования и анализа криптографических протоколов?
Тема 2: Уязвимости и атаки на протоколы
6. Что понимается под уязвимостью криптографического протокола?
7. Какие типы атак наиболее распространены (перехват, повтор, MITM и др.)?
8. Как злоумышленник может использовать утечки данных или ошибки реализации?
9. Как оценивается стойкость протокола к различным типам атак?
10. Как строится формальная модель угроз для криптографического протокола?
Тема 3: Симметричное и асимметричное шифрование в протоколах
11. Как используется симметричное шифрование при построении протоколов?
12. В чём особенности применения асимметричного шифрования?
13. Приведите примеры использования DES, AES, RSA, ElGamal в протоколах.
14. Какие преимущества и недостатки у гибридных схем шифрования?
15. Как обеспечивается совместная работа симметричных и асимметричных методов?
Тема 4: Автоматизация анализа криптографических протоколов
16. Какие подходы используются для автоматического анализа безопасности протоколов?
17. Как работает модель проверки безопасности (BAN-логика)?
18. Какие инструменты применяются для верификации протоколов (ProVerif, Scyther)?
19. Как происходит формальная верификация протоколов на основе логики знаний?
20. Какие цели преследует анализ протоколов на соответствие требованиям безопасности?
Тема 5: Схемы цифровой подписи
21. Что такое цифровая подпись и какие её основные функции?
22. Чем отличаются симметричные и асимметричные схемы подписи?
23. Какие стандарты цифровой подписи используются в России и США (ГОСТ Р 34.10, ECDSA, DSA)?
24. Что такое одноразовая подпись? Примеры: Lamport, Winternitz OTS.
25. Как работают схемы конфиденциальной подписи и подписи вслепую?
Тема 6: Протоколы идентификации
26. Какие задачи решают протоколы идентификации?
27. Что такое парольные протоколы идентификации и их уязвимости?

28. Как работают протоколы типа «запрос-ответ»?
29. Как реализуется идентификация на основе открытого ключа?
30. Что такое протоколы "рукопожатия" и как они используются на практике?
Тема 7: Доказательство знания и нулевое разглашение
31. Что такое интерактивное доказательство и его применение в ИБ?
32. Какие свойства имеет система доказательства с нулевым разглашением?
33. Как работает протокол Фиата-Шамира?
34. Какие практические задачи решаются с помощью ZKP?
35. Как протоколы доказательства знания используются в блокчейн-системах?
Тема 8: Распределение ключей
36. Что такое схемы предварительного распределения ключей?
37. Как работает протокол Блома и где он применяется?
38. Какие схемы используются на основе пересечений множеств?
39. Как работает протокол Диффи–Хеллмана и как его защитить от MITM-атаки?
40. Что такое аутентифицированное распределение ключей и способы его реализации?
Тема 9: Групповые протоколы и разделение секрета
41. Что такое групповой протокол идентификации?
42. Как организуются протоколы разделения секрета (Shamir’s Secret Sharing)?
43. Как работает протокол для телеконференций (conference keying)?
44. Какие требования предъявляются к протоколам группового управления ключами?
45. Как обеспечивается безопасность передачи ключей в многоадресных сетях?
Тема 10: Протоколы битовых обязательств и случайных действий
46. Что такое протокол битового обязательства и как он реализуется?
47. Какие свойства должен иметь протокол битового обязательства?
48. Что такое протокол подбрасывания монеты и как он реализуется?
49. Как организовать игру в покер по телефону с использованием криптографии?
50. Какие задачи решаются с помощью таких протоколов в реальных системах?
Тема 11: Протоколы голосования и электронных денег
51. Какие требования предъявляются к протоколам электронного голосования?
52. Как реализуется конфиденциальность голоса в криптографическом протоколе?
53. Что такое электронные деньги и как они реализуются криптографически?
54. Какие протоколы обеспечивают анонимность и неотслеживаемость?
55. Какие системы используют криптографию для защиты транзакций?
Тема 12: Семейство протоколов KriptoKnight
56. Каково назначение семейства протоколов KriptoKnight?
57. Какие базовые протоколы входят в состав KriptoKnight?
58. Как осуществляется взаимная аутентификация в этих протоколах?
59. Как протоколы KriptoKnight используются в беспроводных сетях?
60. Какие уязвимости могут быть обнаружены в этом семействе?
ема 13: IPsec и связанные протоколы
61. Каково назначение протокола IPsec?
62. Какие компоненты входят в архитектуру IPsec?
63. Как работают протоколы Oakley и ISAKMP?
64. Что представляет собой протокол IKE и как он функционирует?
65. Как обеспечивается безопасность соединений на уровне IP?
Тема 14: Протоколы SSL/TLS и SKIP
66. Как устроен протокол SSL/TLS и какие этапы включает установление соединения?
67. Какие версии TLS считаются безопасными на данный момент?
68. Какие уязвимости были найдены в ранних версиях TLS?
69. Что такое протокол SKIP и чем он отличается от SSL/TLS?
70. Как TLS используется в современных web-приложениях и IoT-устройствах?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Криптографические протоколы" 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: экзамена в 7 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	Васильева И. Н.	Криптографические методы защиты информации: учебник и практикум для вузов	Москва: Юрайт, 2024
Л1.2	Лось А. Б., Нестеренко А. Ю., Рожков М. И.	Криптографические методы защиты информации для изучающих компьютерную безопасность: 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	

		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 "Криптографические протоколы" 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.