МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Методы и средства криптографической защиты информации

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 **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 98,25
самостоятельная работа 45,75

Виды контроля в семестрах:
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	70	70	70	70
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	98,25	98,25	98,25	98,25
Контактная работа	98,25	98,25	98,25	98,25
Сам. работа	45,75	45,75	45,75	45,75
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является формирование у студентов общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов.
1.2	Задачи дисциплины:
1.3	- дать представление об информационной безопасности, как сфере профессиональной деятельности;
1.4	- раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии;
1.5	- ознакомить с основными видами шифров;
1.6	- ознакомить с современными стандартами криптографической защиты;
1.7	- дать представление об атаках на криптографические системы.

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

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:**
3.2	**Уметь:**
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. Введение в криптографию						

1.1	Исторический обзор. Открытые сообщения и их характери-стики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. Основные задачи и понятия криптографииПеречень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
1.2	Шифры замены. Шифр Виженера. Перестановочные шифры. Шифры Хилла /Пр/	6	2	ОПК-10	Л1.1 Л1.2	0	
1.3	Подготовка к практическим занятиям. Выполнение домашних заданий /Ср/	6	22	ОПК-10	Л1.1 Л1.2	0	
	Раздел 2. Криптосистемы с секретным ключом						
2.1	Поточные шифры замены Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, анализ шифра Виженера. Шифры перестановки Разновидности шифровперестановки: маршрутные и геометрические перестановки. Элементы анализа шифров перестановки. /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
2.2	Шифры Хилла. Шифры на основе псевдослучайных последовательностей. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная слож-ность псевдослучайной последовательности. Алгоритм Берлекемпа-Месси. /Лек/	6	2	ОПК-10	Л1.1 Л1.2	0	
2.3	Контрольная работа по симметричным криптосистемам /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
2.4	Шифры на основе линейных рекуррентных последовательностей. Сети Фейстеля. /Пр/	6	6	ОПК-10	Л1.1 Л1.2	2	
2.5	Контрольная работа по теме "Линейные рекуррентные последовательности" /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
2.6	Контрольная работа по теме "Сети Фейстеля" /Пр/	6	2	ОПК-10	Л1.1 Л1.2	1	
	Раздел 3. Криптосистемы с открытым ключом						

3.1	«Public key cryptography»: Принцип построения шифрсистем с открытым ключом. Протокол Диффи-Хеллмана. Шифрсистема на основе задачи об “укладке рюкзака”. Шифрсистема RSA. Шифрсистема Эль-Гамаля. /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
3.2	Шифрсистема Нидеррайтера. Криптосистемы на основе эллиптических кривых. /Лек/	6	2	ОПК-10	Л1.1 Л1.2	0	
3.3	Криптосистема на основе задачи о рюкзаке. Криптосистема RSA /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
3.4	Криптосистема Эль-Гамаля. Эллиптические кривые. Шифрсистемы на основе эллиптических кривых /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
3.5	Контрольная работа по асимметричным системам шифрования. /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
3.6	Элементы криптографического анализа. /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
3.7	Контрольная работа по теме "Криптографический анализ" /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
	Раздел 4. Надежность шифров						
4.1	Основы теории К.Шеннона Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
4.2	Подготовка к зачёту /Ср/	6	10	ОПК-10	Л1.1 Л1.2	0	
	Раздел 5. Алгоритмы цифровой подписи						
5.1	Общие требования к цифровой подписи. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стан-дарты цифровой подписи. /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
5.2	Цифровая подпись Эль-Гамаля. /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
5.3	Цифровая подпись Фиата-Шамира. Цифровая подпись Шнорра. /Пр/	6	6	ОПК-10	Л1.1 Л1.2	1	
5.4	Контрольная работа по теме "Цифровые подписи" /Пр/	6	6	ОПК-10	Л1.1 Л1.2	0	
	Раздел 6. Современные стандарты шифрования						
6.1	Современные блочные шифрсистемы. Сети Фейстеля. Криптоалгоритм DES. Криптоалгоритм RIJNDAEL. Криптоалгоритм ГОСТ-28147-89 /Лек/	6	4	ОПК-10	Л1.1 Л1.2	0	
6.2	Написание программ, реализующих заданные криптоалгоритмы /Ср/	6	13,75	ОПК-10	Л1.1 Л1.2	0	
6.3	Зачет /ИВКР/	6	0,25	ОПК-10	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Исторический обзор криптографии
1. Какова история возникновения криптографии?
2. Какие известны примеры древних шифров?
3. Какие этапы можно выделить в истории развития криптографии как науки?
4. Что такое открытый текст и какие у него статистические характеристики?
5. Как частотные характеристики открытых текстов влияют на криптоанализ?
Тема 2: Основные задачи и понятия криптографии

6. Какие цели преследует современная криптография?
7. Что означают конфиденциальность, целостность, аутентификация и неотказуемость?
8. Какие угрозы существуют в области защиты информации?
9. Каково место криптографии в системе информационной безопасности?
10. Что такое криптографическая система и её компоненты?
Тема 3: Симметричное и асимметричное шифрование
11. Чем отличаются симметричные и асимметричные системы шифрования?
12. В чём преимущества и недостатки каждого подхода?
13. Как происходит распределение ключей в симметричных системах?
14. Как строится модель шифра с открытым ключом?
15. Какие требования предъявляются к криптосистемам?
Тема 4: Классические шифры замены
16. Что такое шифр простой замены и как он реализуется?
17. Как проводится частотный анализ при взломе шифра замены?
18. Как работают многоалфавитные шифры (например, шифр Тритемия)?
19. Как устроен шифр Виженера и как его можно проанализировать?
20. Какие методы применяются для повышения устойчивости шифров замены?
Тема 5: Шифры гаммирования
21. Что такое гаммирование и как оно используется в криптографии?
22. Чем отличается поточный шифр от блочного?
23. Как работает гаммирование с равномерной и неравномерной гаммой?
24. Как повторное использование гаммы влияет на безопасность?
25. Как оценить стойкость шифра Виженера к криптоанализу?
Тема 6: Шифры перестановки
26. Что такое шифр перестановки и как он реализуется?
27. Какие виды перестановочных шифров существуют (маршрутные, табличные)?
28. Как провести криптоанализ шифра перестановки?
29. Какие особенности применения шифров перестановки в практике?
30. Как комбинировать замену и перестановку для повышения стойкости?
Тема 7: Шифры Хилла и псевдослучайные последовательности
31. Как устроен шифр Хилла и какие математические основы положены в его базу?
32. Какие проблемы возникают при использовании шифра Хилла?
33. Что такое псевдослучайная последовательность и где она применяется?
34. Какие свойства имеют линейные рекуррентные последовательности над GF(2)?
35. Как работает алгоритм Берлекемпа-Месси для восстановления ЛРП?
Тема 8: Асимметричная криптография
36. Какова основная идея криптографии с открытым ключом?
37. Как работает протокол Диффи–Хеллмана и как его защитить от MITM-атаки?
38. Как устроена криптосистема RSA? Какие уязвимости у неё есть?
39. Как функционирует криптосистема Эль-Гамаля?
40. Что представляет собой криптосистема Нидеррайтера?
Тема 9: Задача "рюкзака" и эллиптические кривые
41. Как строится криптосистема на основе задачи о рюкзаке?
42. Какие типы задач "рюкзака" являются криптографически стойкими?
43. Какие преимущества даёт использование эллиптических кривых?
44. Как реализуется операция сложения точек на эллиптической кривой?
45. Какие параметры определяют безопасность криптосистем на эллиптических кривых?
Тема 10: Теория Шеннона и теоретическая стойкость
46. Что такое совершенный шифр по Шеннону?
47. Каково значение энтропии в оценке криптостойкости?
48. Что такое одноразовый блокнот и почему он теоретически стоек?
49. Как определить длину ключа, обеспечивающую достаточную стойкость?
50. Как связаны вероятность раскрытия и избыточность открытого текста?
Тема 11: Цифровая подпись
51. Каково назначение цифровой подписи?
52. Как реализуется цифровая подпись на основе RSA?
53. Как работает схема Фиата–Шамира?
54. Как создается и проверяется подпись Эль-Гамаля?
55. Какие стандарты цифровой подписи используются в России и за рубежом (ГОСТ Р 34.10, ECDSA)?
Тема 12: Современные блочные шифры
56. Что такое блочный шифр и как он устроен?
57. Как работает конструкция сети Фейстеля?
58. Как устроен криптоалгоритм DES? Почему он считается устаревшим?
59. Как устроен Rijndael и почему он стал стандартом AES?
60. Как реализован ГОСТ 28147-89 и какие его особенности?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Методы и средства криптографической защиты информации" 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 6 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	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.	Введение в теоретико-числовые методы криптографии: учебное пособие для вузов	Санкт-Петербург: Лань, 2024
Л1.2	Рацеев С. М.	Криптографические методы защиты информации и их основы. Лабораторный практикум: учебное пособие для вузов	Санкт-Петербург: Лань, 2025

6.3.1 Перечень программного обеспечения

6.3.1.1	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.
6.3.1.2	Windows 10	
6.3.1.3	Office Professional Plus 2019	

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	
3-79 А	Специальная библиотека (библиотека литературы ограниченного доступа), предназначенная для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа № 3-79 А	рулонная штора; стол письменный; стул; шкаф металлический (двудверный) для хранения ДСП материалов; шкаф металлический для хранения мобильных телефонов типа ШСТ-26; экраны на батареи.	
3-79	Аудитория (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну № 3-79	рулонные шторы; система виброакустической защиты информации; столы аудиторные для обучающихся, стол преподавателя и стол для размещения компьютера; стулья, доска маркерная; экран; компьютер (в исполнении - моноблок со встроенным или подключаемым DVD/CD-дисководом); проектор; кондиционер; экраны на батареи.	

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).	

6-25	Лаборатория программно-аппаратных средств защиты информации № 6-25	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.	

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

Методические указания по изучению дисциплины "Методы и средства криптографической защиты информации"

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.