МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Методы и средства криптографической защиты информации» предоставить студентам теоретические знания и практические навыки по основам математических подходов к построению современных криптографических алгоритмов.

Задачи изучения дисциплины:

– приобретение студентами знаний, умений и практических навыков, необходимых для изучения основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике;

– выработка основ системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов, изучение принципов синтеза и анализа шифров и математических методов, используемых в криптоанализе.

Дисциплина направлена на формирование общепрофессиональных (ОПК-10) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по направлениям подготовки 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Основы информационной безопасности», «Моделирование угроз информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Управление информационной безопасностью».

Является основой для изучения следующих дисциплин: «Средства и системы технического обеспечения обработки, хранения и передачи информации», «Криптографические протоколы», «Программно-аппаратные средства защиты информации», «Защита и обработка конфиденциальных документов».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения общепрофессиональных задач деятельности, связанных с применением вычислительных систем в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки защищенных информационных систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия и самостоятельная работа студента (72 ак.ч.).

Дисциплина изучается на 3 курсе в 6 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Методы и средства криптографической защиты информации» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10	ОПК-10.1 Анализирует криптографические методы, реализованные в средствах защиты информации ОПК-10.2 Использует средства криптографической защиты информации при решении задач профессиональной деятельности

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к лабораторным занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		6
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	12	12
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	12	12
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	9	9
Работа в библиотеке	9	9
Подготовка к экзамену	21	21
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 4 темы:

– тема 1 (Введение. Основные понятия криптографии);

– тема 2 (Блочные и поточные шифры);

– тема 3 (Шифры с ассиметричным ключом);

- тема 4 (Практические задачи криптографии).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Основные понятия криптографии	Введение. Основные понятия криптографии. Классические шифры: моноалфавитные и полиалфавитные шифры, шифры перестановки.	8	-	-	Хеш-функции	6
2	Блочные и поточные шифры	Блочные и поточные шифры. Шифры с симметричным ключом. Стандарты шифрования. Стандарты DES, AES, ГОСТ.	10	-	-	Комбинированные шифры Шифрование с открытым ключом	6 6
3	Шифры с ассиметричным ключом	Шифры с ассиметричным ключом. Алгоритм RSA.	10	-	-	Протоколы контроля целостности Протоколы электронной цифровой подписи	6 6

Завершение таблицы 3

1	2	3	4	5	6	7	8
4	Практические задачи криптографии	Практические задачи криптографии. Генерация ключей. Алгоритм Диффи-Хеллмана. Алгоритмы хеширования. Электронная цифровая подпись, методы ее конструирования. Электронные деньги.	8	-	-	Протоколы аутентификации и идентификации	6
Всего аудиторных часов		36		-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-10	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– рефераты (2 шт.) – всего 20 баллов;

- практические работы – всего 80 баллов.

Оценка по экзамену проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Методы и средства криптографической защиты информации» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Теоретические основы криптографии

1. История развития криптографии: от древности до наших дней.
2. Математические основы криптографии: теория чисел и конечные поля.
3. Классификация криптографических методов: симметричные и асимметричные системы.
4. Основные задачи криптографии: конфиденциальность, целостность, аутентификация.
5. Понятие криптостойкости и методы криптоанализа.
6. Классы сложности алгоритмов: P, NP, NP-полные задачи.
7. Роль случайности в криптографии: генераторы псевдослучайных чисел.
8. Криптографические протоколы: основные принципы и примеры.
9. Эволюция криптографических стандартов: от DES до постквантовой криптографии.
10. Этические и правовые аспекты использования криптографии.

Симметричные криптографические алгоритмы

11. Принципы работы блочных шифров: структура Фейстеля.
12. Алгоритм DES: история, принципы работы и уязвимости.
13. Алгоритм AES: особенности и преимущества перед DES.
14. ГОСТ 28147-89: российский стандарт шифрования.
15. Режимы работы блочных шифров: ECB, CBC, CFB, OFB, CTR.
16. Потоковые шифры: принципы работы и примеры (RC4, Salsa20).
17. Криптоанализ симметричных алгоритмов: методы и примеры.
18. Дифференциальный и линейный криптоанализ: принципы и применение.

19. Сравнение блочных и потоковых шифров: преимущества и недостатки.

20. Атаки на симметричные шифры: полный перебор и атаки по времени.

Асимметричные криптографические алгоритмы

21. Принципы работы асимметричной криптографии.

22. Алгоритм RSA: математические основы и применение.

23. Уязвимости RSA: атаки на малый модуль и слабые ключи.

24. Алгоритм Эль-Гамаля: принципы работы и применение.

25. Эллиптические кривые в криптографии: преимущества и примеры.

26. Алгоритм ECDSA: цифровые подписи на эллиптических кривых.

27. Протокол Диффи-Хеллмана: обмен ключами в асимметричной криптографии.

28. Криптоанализ асимметричных алгоритмов: методы и примеры.

29. Сравнение RSA и ECC: производительность и безопасность.

30. Постквантовая криптография: алгоритмы, устойчивые к квантовым атакам.

Хэш-функции и цифровые подписи

31. Принципы работы криптографических хэш-функций.

32. Алгоритмы хэширования: SHA-1, SHA-2, SHA-3.

33. Российский стандарт хэширования: ГОСТ Р 34.11-2012.

34. Применение хэш-функций в цифровых подписях.

35. Цифровые подписи: принципы работы и примеры (RSA, DSA, ECDSA).

36. Российский стандарт цифровых подписей: ГОСТ Р 34.10-2012.

37. Атаки на хэш-функции: коллизии и методы их поиска.

38. Применение хэш-функций в блокчейне.

39. Цифровые подписи в электронных документах: преимущества и риски.

40. Квантовые угрозы для хэш-функций и цифровых подписей.

Криптографические протоколы

41. Протокол SSL/TLS: принципы работы и применение.

42. Атаки на протокол TLS: BEAST, CRIME, POODLE.

43. Протокол IPSec: защита сетевого уровня.

44. Протокол Kerberos: аутентификация в распределенных системах.

45. Протоколы обмена ключами: Diffie-Hellman, ECDH.

46. Протоколы аутентификации: OAuth, OpenID.

47. Криптографические протоколы в электронной почте: PGP, S/MIME.

48. Протоколы защиты данных в облачных сервисах.
49. Криптографические протоколы в IoT: проблемы и решения.
50. Протоколы квантовой криптографии: BB84, E91.

Криптография в современных технологиях

51. Криптография в блокчейне: принципы и применение.
52. Криптографические алгоритмы в Bitcoin и Ethereum.
53. Криптография в облачных технологиях: шифрование данных и ключей.
54. Криптография в IoT: защита устройств и данных.
55. Криптография в мобильных приложениях: безопасность данных.
56. Криптография в социальных сетях: защита конфиденциальности.
57. Криптография в электронных платежных системах.
58. Криптография в системах голосования: обеспечение безопасности.
59. Криптография в медицинских системах: защита персональных данных.
60. Криптография в системах умного дома: проблемы и решения.

Квантовая криптография

61. Принципы квантовой криптографии.
62. Протокол BB84: квантовое распределение ключей.
63. Угрозы квантовых компьютеров для классической криптографии.
64. Постквантовая криптография: алгоритмы и стандарты.
65. Квантовые хэш-функции: принципы и применение.
66. Квантовые цифровые подписи: преимущества и ограничения.
67. Квантовые сети: принципы работы и применение.
68. Квантовая криптография в системах связи.
69. Квантовые угрозы для блокчейна.
70. Будущее квантовой криптографии: перспективы и вызовы.

Криптоанализ и уязвимости

71. Методы криптоанализа: полный перебор, атаки по времени.
72. Атаки на симметричные шифры: дифференциальный и линейный криптоанализ.
73. Атаки на асимметричные шифры: факторизация и дискретный логарифм.
74. Атаки на хэш-функции: коллизии и методы их поиска.
75. Атаки на криптографические протоколы: примеры и защита.
76. Уязвимости в реализации криптографических алгоритмов.
77. Атаки на блокчейн: двойное расходование и атаки 51%.
78. Уязвимости в IoT: проблемы криптографической защиты.
79. Атаки на облачные сервисы: утечки данных и ключей.

80. Социальная инженерия и криптография: методы защиты.

Стандарты и сертификация

81. Криптографические стандарты: ГОСТ, NIST, FIPS.

82. Сертификация криптографических средств: процедуры и требования.

83. Российские стандарты криптографии: ГОСТ 28147-89, ГОСТ Р 34.10-2012.

84. Международные стандарты криптографии: AES, RSA, ECC.

85. Стандарты постквантовой криптографии: NIST PQC.

86. Криптографические стандарты в банковской сфере.

87. Стандарты защиты данных в облачных сервисах.

88. Криптографические стандарты в IoT.

89. Стандарты защиты данных в медицинских системах.

90. Будущее криптографических стандартов: тенденции и вызовы.

Прикладные аспекты криптографии

91. Криптография в системах электронного документооборота.

92. Криптография в системах защиты авторских прав.

93. Криптография в системах защиты персональных данных.

94. Криптография в системах защиты коммерческой тайны.

95. Криптография в системах защиты государственной тайны.

96. Криптография в системах защиты военных данных.

97. Криптография в системах защиты финансовых данных.

98. Криптография в системах защиты данных в социальных сетях.

99. Криптография в системах защиты данных в играх.

100. Криптография в системах защиты данных в образовании.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

*Тема 1 (*Основные понятия криптографии*)*

Базовые тесты (10)

1. Что такое криптография?

a) Наука о создании вирусов

b) Наука о защите информации с помощью математических методов

c) Наука о создании операционных систем

d) Наука о проектировании сетей

Ответ: b) Наука о защите информации с помощью математических методов

2. Какая задача криптографии обеспечивает невозможность отказа от

авторства?

a) Конфиденциальность

b) Целостность

c) Аутентификация

d) Неотрекаемость

Ответ: d) Неотрекаемость

3. Что такое открытый текст?

a) Зашифрованные данные

b) Исходные данные, которые нужно защитить

c) Ключ для шифрования

d) Алгоритм шифрования

Ответ: b) Исходные данные, которые нужно защитить

4. Какой алгоритм является симметричным?

a) RSA

b) AES

c) ECC

d) DSA

Ответ: b) AES

5. Что такое криптостойкость?

a) Скорость шифрования

b) Устойчивость алгоритма к взлому

c) Длина ключа

d) Количество раундов шифрования

Ответ: b) Устойчивость алгоритма к взлому

6. Какой режим работы блочных шифров использует вектор инициализации?

a) ECB

b) CBC

c) CFB

d) OFB

Ответ: b) CBC

7. Что такое хэш-функция?

a) Алгоритм для шифрования данных

b) Алгоритм для создания цифровой подписи

c) Алгоритм для преобразования данных в фиксированную длину

d) Алгоритм для обмена ключами

Ответ: c) Алгоритм для преобразования данных в фиксированную длину

8. Какой алгоритм используется для цифровой подписи?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

9. Что такое криптоанализ?

a) Наука о создании криптографических алгоритмов

b) Наука о взломе криптографических алгоритмов

c) Наука о создании сетей

d) Наука о защите данных

Ответ: b) Наука о взломе криптографических алгоритмов

10. Какой стандарт описывает алгоритм ГОСТ 28147-89?

a) Российский стандарт шифрования

b) Американский стандарт шифрования

c) Европейский стандарт шифрования

d) Международный стандарт шифрования

Ответ: a) Российский стандарт шифрования

Тесты повышенного уровня (7)

1. В шифре Цезаря каждый символ открытого текста заменяется на символ, находящийся на ___ позиций в алфавите.

Ответ: фиксированное число

2. В режиме ___ блочного шифра каждый блок шифруется независимо.

Ответ: ECB

3. Алгоритм RSA основан на сложности задачи ___ больших чисел.

Ответ: факторизации

4. В алгоритме Диффи-Хеллмана ключ вычисляется как ___ от общего секрета.

Ответ: степень

5. Хэш-функция SHA-256 создает хэш длиной ___ бит.

Ответ: 256

6. В цифровой подписи ECDSA используется ___ кривые.

Ответ: эллиптические

7. Криптоанализ, основанный на изучении времени выполнения операций, называется ___ атакой.

Ответ: временной

Тесты высокого уровня (3)

1. Напишите формулу для шифра Цезаря:

Ответ: $C = (P + K) \bmod 26$, где C — шифротекст, P — открытый текст, K — ключ.

2. Напишите формулу для вычисления открытого ключа в RSA:

Ответ: e * d ≡ 1 mod φ(n), где e — открытый ключ, d — закрытый ключ, φ(n) — функция Эйлера.

3. Дайте определение криптостойкости:

Ответ: Криптостойкость — это свойство криптографического алгоритма противостоять попыткам взлома.

*Тема 2 (*Блочные и поточные шифры*)*

Базовые тесты (10)

1. Какой алгоритм является блочным шифром?

a) RC4

b) AES

c) RSA

d) ECC

Ответ: b) AES

2. Какой режим работы блочных шифров использует XOR с предыдущим блоком?

a) ECB

b) CBC

c) CFB

d) OFB

Ответ: b) CBC

3. Какой алгоритм является потоковым шифром?

a) AES

b) DES

c) RC4

d) RSA

Ответ: c) RC4

4. Какой размер блока у алгоритма AES?

a) 64 бита

b) 128 бит

c) 256 бит

d) 512 бит

Ответ: b) 128 бит

5. Какой режим работы блочных шифров не использует вектор инициализации?

a) ECB

b) CBC

c) CFB

d) OFB

Ответ: a) ECB

6. Какой алгоритм использует структуру Фейстеля?

a) AES

b) DES

c) RSA

d) ECC

Ответ: b) DES

7. Какой размер ключа у алгоритма ГОСТ 28147-89?

a) 128 бит

b) 192 бит

c) 256 бит

d) 512 бит

Ответ: c) 256 бит

8. Какой режим работы блочных шифров использует обратную связь по шифротексту?

a) ECB

b) CBC

c) CFB

d) OFB

Ответ: c) CFB

9. Какой алгоритм является потоковым шифром?

a) AES

b) DES

c) RC4

d) RSA

Ответ: c) RC4

10. Какой режим работы блочных шифров использует обратную связь по выходу?

a) ECB

b) CBC

c) CFB

d) OFB

Ответ: d) OFB

Тесты повышенного уровня (7)

1. В режиме ___ блочного шифра каждый блок шифруется независимо.

Ответ: ECB

2. В режиме ___ блочного шифра используется вектор инициализации.

Ответ: CBC

3. В потоковых шифрах каждый бит открытого текста шифруется ___ с битом ключевого потока.

Ответ: XOR

4. В алгоритме AES количество раундов зависит от ___.

Ответ: длины ключа

5. В алгоритме DES используется ___ раундов.

Ответ: 16

6. В режиме ___ блочного шифра используется обратная связь по шифротексту.

Ответ: CFB

7. В режиме ___ блочного шифра используется обратная связь по выходу.

Ответ: OFB

Тесты высокого уровня (3)

1. Напишите формулу для шифрования в режиме CBC:

Ответ: C_i = E_k(P_i ⊕ C_{i-1}), где C_i — шифротекст, P_i — открытый текст, E_k — функция шифрования, C_{i-1} — предыдущий блок шифротекста.

2. Напишите формулу для генерации ключевого потока в RC4:

Ответ: K_i = S[(S[i] + S[j]) mod 256], где S — массив состояний, i и j — индексы.

3. Дайте определение структуры Фейстеля:

Ответ: Структура Фейстеля — это метод построения блочных шифров, при котором блок данных разделяется на две части, которые обрабатываются отдельно и затем объединяются.

*Тема 3 (*Шифры с ассиметричным ключом*)*

Базовые тесты (10)

1. Какой алгоритм является асимметричным?

a) AES

b) RSA

c) DES

d) RC4

Ответ: b) RSA

2. Какой алгоритм используется для обмена ключами?

a) RSA

b) Диффи-Хеллман

c) AES

d) DES

Ответ: b) Диффи-Хеллман

3. Какой алгоритм используется для цифровой подписи?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

4. Какой алгоритм основан на сложности задачи дискретного логарифма?

a) RSA

b) Диффи-Хеллман

c) AES

d) DES

Ответ: b) Диффи-Хеллман

5. Какой алгоритм использует эллиптические кривые?

a) RSA

b) ECDSA

c) AES

d) DES

Ответ: b) ECDSA

6. Какой размер ключа рекомендуется для RSA?

a) 1024 бита

b) 2048 бит

c) 4096 бит

d) 8192 бит

Ответ: b) 2048 бит

7. Какой алгоритм используется для шифрования в асимметричных системах?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

8. Какой алгоритм используется для цифровой подписи на эллиптических кривых?

a) RSA

b) ECDSA

c) AES

d) DES

Ответ: b) ECDSA

9. Какой алгоритм используется для обмена ключами на эллиптических кривых?

a) RSA

b) ECDH

c) AES

d) DES

Ответ: b) ECDH

10. Какой алгоритм используется для шифрования в асимметричных системах?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

Тесты повышенного уровня (7)

1. В алгоритме RSA открытый ключ вычисляется как ___ от закрытого ключа.

Ответ: обратный

2. В алгоритме Диффи-Хеллмана ключ вычисляется как ___ от общего секрета.

Ответ: степень

3. В алгоритме ECDSA используется ___ кривые.

Ответ: эллиптические

4. В алгоритме RSA закрытый ключ вычисляется как ___ от открытого ключа.

Ответ: обратный

5. В алгоритме Диффи-Хеллмана ключ вычисляется как ___ от общего секрета.

Ответ: степень

6. В алгоритме ECDSA используется ___ кривые.

Ответ: эллиптические

7. В алгоритме RSA закрытый ключ вычисляется как ___ от открытого ключа.

Ответ: обратный

Тесты высокого уровня (3)

1. Напишите формулу для вычисления открытого ключа в RSA:

Ответ: $e * d \equiv 1 \mod \varphi(n)$, где e — открытый ключ, d — закрытый ключ, $\varphi(n)$ — функция Эйлера.

2. Напишите формулу для вычисления общего ключа в алгоритме Диффи-Хеллмана:

Ответ: K = g^{ab} mod p, где K — общий ключ, g — генератор, a и b — секретные ключи, p — простое число.

3. Дайте определение эллиптической кривой:

Ответ: Эллиптическая кривая — это множество точек, удовлетворяющих уравнению y^2 = x^3 + ax + b, где a и b — коэффициенты.

*Тема 4 (*Практические задачи криптографии*)*

Базовые тесты (10)

1. Какой алгоритм используется для защиты данных в TLS?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: a) AES

2. Какой алгоритм используется для цифровой подписи в TLS?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

3. Какой алгоритм используется для хэширования в TLS?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: c) SHA-256

4. Какой алгоритм используется для обмена ключами в TLS?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

5. Какой алгоритм используется для защиты данных в IPSec?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: a) AES

6. Какой алгоритм используется для цифровой подписи в IPSec?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

7. Какой алгоритм используется для хэширования в IPSec?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: c) SHA-256

8. Какой алгоритм используется для обмена ключами в IPSec?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

9. Какой алгоритм используется для защиты данных в SSH?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: a) AES

10. Какой алгоритм используется для цифровой подписи в SSH?

a) AES

b) RSA

c) SHA-256

d) RC4

Ответ: b) RSA

Тесты повышенного уровня (7)

1. В протоколе TLS используется ___ для защиты данных.

Ответ: AES

2. В протоколе TLS используется ___ для цифровой подписи.

Ответ: RSA

3. В протоколе TLS используется ___ для хэширования.

Ответ: SHA-256

4. В протоколе TLS используется ___ для обмена ключами.

Ответ: RSA

5. В протоколе IPSec используется ___ для защиты данных.

Ответ: AES

6. В протоколе IPSec используется ___ для цифровой подписи.

Ответ: RSA

7. В протоколе IPSec используется ___ для хэширования.

Ответ: SHA-256

Тесты высокого уровня (3)

1. Напишите формулу для вычисления общего ключа в алгоритме Диффи-Хеллмана:

Ответ: K = g^{ab} mod p, где K — общий ключ, g — генератор, a и b — секретные ключи, p — простое число.

2. Напишите формулу для вычисления открытого ключа в RSA:

Ответ: e * d ≡ 1 mod φ(n), где e — открытый ключ, d — закрытый ключ, φ(n) — функция Эйлера.

3. Дайте определение эллиптической кривой:

Ответ: Эллиптическая кривая — это множество точек, удовлетворяющих уравнению y^2 = x^3 + ax + b, где a и b — коэффициенты.

6.5 Вопросы для подготовки к экзамену

1. Дайте определение криптографии. Какие основные задачи она решает?
2. Что такое симметричные и асимметричные криптосистемы? В чем их основные различия?
3. Опишите принцип работы шифра Цезаря.
4. Что такое криптостойкость? Какие факторы на нее влияют?
5. Опишите структуру Фейстеля в блочных шифрах.
6. Какие режимы работы блочных шифров вы знаете? Опишите ECB и CBC.
7. Что такое потоковые шифры? Приведите примеры.
8. Опишите алгоритм RSA. Какие математические основы он использует?
9. Что такое эллиптические кривые в криптографии? Какие преимущества они имеют перед RSA?
10. Опишите принцип работы алгоритма Диффи-Хеллмана.
11. Что такое хэш-функция? Какие требования к ней предъявляются?
12. Опишите алгоритмы SHA-2 и SHA-3. В чем их различия?
13. Что такое цифровая подпись? Какие алгоритмы используются для ее создания?
14. Опишите принцип работы протокола TLS.

15. Что такое квантовая криптография? Какие угрозы она устраняет?
16. Опишите протокол BB84 для квантового распределения ключей.
17. Что такое постквантовая криптография? Какие алгоритмы в нее входят?
18. Опишите принцип работы алгоритма AES.
19. Что такое криптоанализ? Какие методы криптоанализа вы знаете?
20. Опишите принцип работы алгоритма ГОСТ 28147-89.
21. Что такое атака "человек посередине" (Man-in-the-Middle)? Как от нее защититься?
22. Опишите принцип работы алгоритма Эль-Гамаля.
23. Что такое коллизия в хэш-функциях? Почему это важно?
24. Опишите принцип работы алгоритма ECDSA.
25. Что такое криптографический протокол? Приведите примеры.
26. Почему режим ECB не рекомендуется для шифрования изображений?
27. В чем преимущество асимметричных криптосистем перед симметричными?
28. Почему длина ключа важна для безопасности шифра?
29. Как работает атака полным перебором? В каких случаях она эффективна?
30. Почему эллиптические кривые считаются более эффективными, чем RSA?
31. Как можно защититься от атаки на малый модуль в RSA?
32. Почему хэш-функции используются для проверки целостности данных?
33. Как работает атака на повторное использование ключа в RC4?
34. Почему квантовые компьютеры угрожают классической криптографии?
35. Как протокол TLS обеспечивает конфиденциальность и целостность данных?
36. Почему цифровые подписи важны для электронных документов?
37. Как работает атака "дней рождения" на хэш-функции?
38. Почему режим CBC более безопасен, чем ECB?
39. Как можно защититься от атаки "человек посередине" в протоколе Диффи-Хеллмана?
40. Почему постквантовая криптография важна для будущего?
41. Как работает атака на слабые ключи в DES?
42. Почему хэш-функции используются в блокчейне?

43. Как можно защититься от атаки на повторное использование nonce в AES-GCM?

44. Почему криптографические протоколы важны для IoT?

45. Как работает атака на повторное использование IV в WEP?

46. Почему криптография важна для облачных технологий?

47. Как можно защититься от атаки на повторное использование ключа в потоковых шифрах?

48. Почему криптография важна для блокчейна?

49. Как работает атака на слабые параметры в ECDSA?

50. Почему криптографические стандарты важны для безопасности?

51. Зашифруйте текст "HELLO" с использованием шифра Цезаря с ключом 3.

52. Расшифруйте текст "KHOOR", зашифрованный шифром Цезаря с ключом 3.

53. Зашифруйте текст "CRYPTO" с использованием шифра Виженера и ключа "KEY".

54. Реализуйте алгоритм RSA для шифрования числа 42 с открытым ключом (e=17, n=3233).

55. Реализуйте алгоритм RSA для расшифрования числа 2557 с закрытым ключом (d=2753, n=3233).

56. Вычислите хэш-значение для строки "Hello, World!" с использованием SHA-256.

57. Проверьте, является ли хэш-значение "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824" корректным для строки "hello".

58. Реализуйте алгоритм Диффи-Хеллмана для обмена ключами с параметрами p=23, g=5, a=6, b=15.

59. Зашифруйте текст "SECRET" с использованием AES в режиме ECB.

60. Расшифруйте текст, зашифрованный AES в режиме CBC, с ключом и вектором инициализации.

61. Реализуйте алгоритм цифровой подписи ECDSA для сообщения "Test".

62. Проверьте цифровую подпись ECDSA для сообщения "Test" с предоставленными параметрами.

63. Реализуйте алгоритм хэширования ГОСТ Р 34.11-2012 для строки "Hello".

64. Проверьте целостность файла, используя хэш-функцию SHA-256.

65. Реализуйте протокол TLS для установления защищенного соединения.

66. Проведите атаку полным перебором на шифр Цезаря для зашифрованного текста "KHOOR".

67. Реализуйте атаку на малый модуль в RSA для зашифрованного текста.

68. Проведите частотный анализ для взлома шифра Виженера.

69. Реализуйте алгоритм Эль-Гамаля для шифрования числа 42.

70. Проверьте цифровую подпись RSA для сообщения "Test" с предоставленными параметрами.

71. Реализуйте алгоритм AES для шифрования изображения в режиме CBC.

72. Проведите атаку на повторное использование ключа в RC4.

73. Реализуйте протокол BB84 для квантового распределения ключей.

74. Проверьте целостность данных с использованием хэш-функции SHA-3.

75. Реализуйте алгоритм цифровой подписи DSA для сообщения "Test".

Вопросы по криптоанализу

1. Что такое криптоанализ? Какие основные задачи он решает?
2. Какие виды криптоанализа вы знаете? Опишите каждый из них.
3. Что такое атака с известным открытым текстом (Known Plaintext Attack)?
4. Что такое атака с выбранным открытым текстом (Chosen Plaintext Attack)?
5. Что такое атака с выбранным шифротекстом (Chosen Ciphertext Attack)?
6. Что такое атака на основе подобранного текста (Adaptive Chosen Plaintext Attack)?
7. Что такое атака "дней рождения"? Как она применяется в криптоанализе?
8. Что такое дифференциальный криптоанализ? На каких принципах он основан?
9. Что такое линейный криптоанализ? Как он работает?
10. Что такое атака по времени (Timing Attack)? Как от нее защититься?
11. Что такое атака по сторонним каналам (Side-Channel Attack)? Приведите примеры.

12. Что такое атака на слабые ключи? Приведите примеры алгоритмов, уязвимых к таким атакам.

13. Что такое атака на повторное использование nonce? Как она применяется в AES-GCM?

14. Что такое атака на повторное использование ключа в потоковых шифрах?

15. Что такое атака на малый модуль в RSA? Как от нее защититься?

16. Почему атака полным перебором эффективна только для коротких ключей?

17. Как дифференциальный криптоанализ применяется для взлома DES?

18. Почему линейный криптоанализ эффективен против некоторых блочных шифров?

19. Как атака "дней рождения" используется для поиска коллизий в хэш-функциях?

20. Почему атака по времени опасна для реализации RSA?

21. Как атака по сторонним каналам может быть использована для взлома AES?

22. Почему атака на слабые ключи возможна в DES?

23. Как атака на повторное использование nonce может привести к утечке данных в AES-GCM?

24. Почему атака на повторное использование ключа опасна для потоковых шифров?

25. Как атака на малый модуль в RSA может привести к взлому шифра?

26. Проведите атаку полным перебором на шифр Цезаря для зашифрованного текста "KHOOR".

27. Проведите частотный анализ для взлома шифра Виженера с зашифрованным текстом "LXFOPVEFRNHR".

28. Проведите дифференциальный криптоанализ на упрощенной версии DES.

29. Проведите линейный криптоанализ на упрощенной версии AES.

30. Проведите атаку "дней рождения" для поиска коллизий в хэш-функции SHA-1.

31. Проведите атаку по времени на реализацию RSA.

32. Проведите атаку по сторонним каналам на реализацию AES.

33. Проведите атаку на слабые ключи в DES.

34. Проведите атаку на повторное использование nonce в AES-GCM.

35. Проведите атаку на повторное использование ключа в RC4.

36. Проведите атаку на малый модуль в RSA для зашифрованного текста.

37. Проведите атаку на повторное использование IV в WEP.

38. Проведите атаку на слабые параметры в ECDSA.

39. Проведите атаку на повторное использование ключа в потоковом шифре Salsa20.

40. Проведите атаку на повторное использование nonce в ChaCha20.

41. Проведите атаку на слабые ключи в ГОСТ 28147-89.

42. Проведите атаку на повторное использование ключа в алгоритме Эль-Гамаля.

43. Проведите атаку на повторное использование nonce в алгоритме RSA-OAEP.

44. Проведите атаку на повторное использование ключа в алгоритме Диффи-Хеллмана.

45. Проведите атаку на слабые параметры в алгоритме DSA.

46. Проведите атаку на повторное использование ключа в алгоритме ECDSA.

47. Проведите атаку на повторное использование nonce в алгоритме EdDSA.

48. Проведите атаку на слабые ключи в алгоритме ГОСТ Р 34.10-2012.

49. Проведите атаку на повторное использование ключа в алгоритме ГОСТ Р 34.11-2012.

50. Проведите атаку на слабые параметры в алгоритме ГОСТ Р 34.10-2012.

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Владимиров, С. М. Криптографические методы защиты информации. Учебное пособие. [Электронный ресурс], 2021. – 433 с., ил. – Режим доступа: https://github.com/vlsergey/infosec/releases/tag/v2021.11.06. (Дата обращения 26.08.2023).

2. Бутакова, Н.Г. Криптографические методы и средства защиты информации: учеб. пособие / Н.Г.Бутакова, Н.В.Федоров. − СПб.: ИЦ «Интермедия», 2019. – 384 с. – Режим доступа: https://obuchalka.org/20190604109900/kriptograficheskie-metodi-i-sredstva-zaschiti-informacii-uchebnoe-posobie-butakova-n-g-fedorov-n-v-2019.htm. 1 (Дата обращения 26.08.2023).

3. Запечников, С.В. Криптографические методы защиты информации: учебник для вузов / С.В. Запечников, О.В. Казарин, А.А. Тарасов. – Москва: Издательство Юрайт, 2022. – 309 с. - Режим доступа: https://vk.com/wall-206723877_9876. (Дата обращения 26.08.2023).

4. Омассон, Ж.-Ф. О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2021. – 328 с.: ил. - Режим доступа: https://vk.com/topic-51126445_36360999. (Дата обращения 26.08.2023).

5. Свейгарт, Эл Криптография и взлом шифров на Python. : Пер. с англ. - СПб.: ООО" Диалектика", 2020. - 512 с. - Парал. тит. англ – Режим доступа: https://vk.com/doc44301783_616532398?hash=p3kYBn0zYd0581qp2mxN5FuCinOUwP3eyncEM8siKzz. (Дата обращения: 26.08.2023).

6. Граймс, Р. А. Апокалипсис криптографии / пер. с англ. В. А. Яроцкого. – М.: ДМК Пресс, 2020. – 290 с.: ил – Режим доступа: https://vk.com/doc44301783_561673685?hash=sc28jNQ4G8SkDKih3vECProycHttGh9ZBjLEPFG7dzP. (Дата обращения 26.08.2023).

Дополнительная литература

1. Методы и средства криптографической защиты информации [Текст] / Методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» /В.А.Алексеев, Липецк: ЛГТУ, 2009. –16 с.—опубл. 17.10.2013. — Электрон. версия печ. публ.—Доступ с сайта ЭБС IPRbooks. // Режим доступа: https://www.iprbookshop.ru/epd-reader?publicationId=17710. (Дата обращения: 26.08.2023).

2. Menezes A. Handbook of Applied Cryptography, by A. Menezes, P. van

Oorschot, and S. Vanstone, CRC Press, 1996. – 780c. - Режим доступа: https://cacr.uwaterloo.ca/hac/. (Дата обращения 26.08.2023).

Учебно-методические материалы и пособия

1. Методы и средства защиты информации в компьютерных системах: лабораторный практикум : [для студ. напр. подготовки 09.04.01 «Информатика и вычислительная техника» 6 курса всех форм обучения] / сост. А.С. Закутный ; Каф. Специализированных компьютерных систем . ─ Алчевск : ГОУ ВО ЛНР ДонГТИ, 2021 . ─ 155 с. – Режим доступа: https://library.dontu.ru/download.php?rec=123183 (Дата обращения 26.08.2023).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education. — Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/. — Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x. — Текст : электронный.
4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red. – Текст : электронный.
5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: http://www.iprbookshop.ru/. — Текст : электронный.
6. Сайт кафедры ИСИБ http://scs.dstu.education.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций:	ауд. *207* корп. *4*
Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) А.С. Закутный
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Протокол №__1__ заседания кафедры от __27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической комиссии по специальности Информационная безопасность автоматизированных систем	10.05.03	(подпись)	Е.Е. Бизянов (Ф.И.О.)

Начальник учебно-методического центра (подпись) О.А. Коваленко (Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>