



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.04 МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ
ИНФОРМАЦИИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 8 з.е.
в академических часах: 288 ак.ч.

Москва, 2024

Разработчики:

Декан факультета кафедры Информационно-измерительных систем, д.т.н. Матерухин А. В.

Старший преподаватель кафедры
Информационно-измерительных систем Бельшева Ю. В.

Преподаватель кафедры Информационно-измерительных систем
Калмыков С. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся теоретических знаний и практических навыков в области применения современных методов и средств криптографической защиты информации для обеспечения конфиденциальности, целостности и подлинности данных в информационных системах

Задачи изучения дисциплины:

- сформировать понимание математических основ криптографии и принципов построения криптографических алгоритмов и протоколов;
- обучить анализу и выбору методов криптографической защиты информации в зависимости от требований безопасности и условий функционирования информационных систем;
- развить навыки практического применения криптографических средств защиты информации, включая оценку их стойкости и корректности использования.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

ОПК-9.1 Знает основные характеристики, достоинства и недостатки средств криптографической и технической защиты информации в автоматизированных системах

Знать:

ОПК-9.1/Зн1 Основные виды угроз безопасности информации в автоматизированных системах и способов противодействия им

ОПК-9.1/Зн2 Характеристики симметричных и асимметричных алгоритмов шифрования, хэш-функций и электронных подписей

ОПК-9.1/Зн3 Нормативные требования и стандарты в области криптографической защиты информации

Уметь:

ОПК-9.1/Ум1 Анализировать характеристики и ограничения средств криптографической защиты информации

Владеть:

ОПК-9.1/Нв1 Терминологическим аппаратом в области криптографической защиты информации

ОПК-9.2 Применяет средства криптографической и технической защиты информации от «утечки»

Знать:

ОПК-9.2/Зн1 Методы криптографической защиты информации при передаче и хранении данных

Уметь:

ОПК-9.2/Ум1 Применять криптографические средства для защиты информации

ОПК-9.2/Ум2 Реализовывать механизмы шифрования, аутентификации и контроля целостности данных

Владеть:

ОПК-9.2/Нв1 Навыками практического применения криптографических алгоритмов и протоколов

ОПК-9.3 Применяет технические средства контроля эффективности применяемых мер защиты информации

Знать:

ОПК-9.3/Зн1 Методы и средства контроля эффективности мер защиты информации

Уметь:

ОПК-9.3/Ум1 Проводить контроль эффективности применяемых криптографических и технических мер защиты

Владеть:

ОПК-9.3/Нв1 Техническими средствами контроля защищенности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.04 «Методы и средства криптографической защиты информации» относится к обязательной части образовательной программы и изучается в семестре(ах): 5, 6.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
5 семестр	144	4	34	34	76	Зачет с оценкой
6 семестр	144	4		36	72	Экзамен (36)
Всего	288	8	34	70	148	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы

Раздел 1. Введение в криптографию. Основные понятия и определения	48	11	11	26	ОПК-9.1
Тема 1.1. Криптоанализ шифра Виженера	24	5	5	14	
Тема 1.2. Криптоанализ шифра Вернама при условии неоднократного использования одинакового ключа	24	6	6	12	
Раздел 2. Математические основы криптографии	50	12	12	26	ОПК-9.1 ОПК-9.2
Тема 2.1. Схема Диффи–Хеллмана	26	6	6	14	
Тема 2.2. Криптоанализ алгоритма RSA в базовой форме	24	6	6	12	
Раздел 3. Стойкость криптоалгоритмов	46	11	11	24	ОПК-9.2 ОПК-9.3
Тема 3.1. Атака с выбором открытого текста	24	6	6	12	
Тема 3.2. Атака с выбором зашифрованного текста	22	5	5	12	
Раздел 4. Поточные шифры	16		5	11	ОПК-9.2
Тема 4.1. Линейные регистры сдвига с обратной связью (LFSR) и их криптоанализ	16		5	11	
Раздел 5. Блочные шифры	46		15	31	ОПК-9.2 ОПК-9.3
Тема 5.1. Режимы шифрования блочных шифров	15		5	10	
Тема 5.2. Схема CBC-MAC	16		5	11	
Тема 5.3. Реализация атаки на CBC-MAC	15		5	10	
Раздел 6. Криптографические протоколы	16		6	10	ОПК-9.1
Тема 6.1. Схема идентификации Шнорра	16		6	10	
Раздел 7. Построение криптографических примитивов	30		10	20	ОПК-9.2 ОПК-9.3
Тема 7.1. Реализация атаки на алгоритм RSA в базовой форме	15		5	10	
Тема 7.2. Хэш-функции и коллизии	15		5	10	
Итого	252	34	70	148	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Введение в криптографию. Основные понятия и определения

Тема 1.1. Криптоанализ шифра Виженера

Понятие классических шифров. Полиалфавитное шифрование. Метод Касиски и индекс совпадений

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Криптоанализ шифра Вернама при условии неоднократного использования одинакового ключа

Частотный анализ. Принцип одноразового блокнота. Условия абсолютной стойкости. Уязвимости при повторном использовании гаммы

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Математические основы криптографии

Тема 2.1. Схема Диффи–Хеллмана

Арифметика по модулю. Теория чисел. Дискретное логарифмирование. Вычислительная сложность задач

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Криптоанализ алгоритма RSA в базовой форме

Проблема факторизации больших чисел. Выбор параметров RSA. Типовые математические уязвимости

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 3. Стойкость криптоалгоритмов

Тема 3.1. Атака с выбором открытого текста

Модели криптоаналитических атак. Понятие криптографической стойкости. Адаптивные атаки

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.2. Атака с выбором зашифрованного текста

Практические сценарии реализации атак. Оценка устойчивости алгоритмов к активному криптоанализу

Текущий контроль

Вид (форма) контроля

Тестирование

Раздел 4. Поточные шифры

Тема 4.1. Линейные регистры сдвига с обратной связью (LFSR) и их криптоанализ

Принципы построения потоковых шифров. Генерация гаммы. Линейные регистры сдвига с обратной связью. Характеристический многочлен. Линейная сложность последовательности. Алгоритм Берлекэмпа–Мэсси. Методы повышения стойкости потоковых шифров. Анализ уязвимостей линейных генераторов

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 5. Блочные шифры

Тема 5.1. Режимы шифрования блочных шифров

Структура блочных шифров

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 5.2. Схема CBC-MAC

Режимы ECB, CBC, CFB, OFB, CTR. Принципы аутентификации сообщений

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 5.3. Реализация атаки на CBC-MAC

Построение CBC-MAC. Условия корректного применения. Типовые атаки на MAC-схемы

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 6. Криптографические протоколы

Тема 6.1. Схема идентификации Шнорра

Протоколы аутентификации. Доказательство знания без раскрытия секрета. Параметры схемы Шнорра. Анализ устойчивости к атакам повторного воспроизведения

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 7. Построение криптографических примитивов

Тема 7.1. Реализация атаки на алгоритм RSA в базовой форме

Понятие криптографического примитива. Требования к примитивам. Свойства криптографических хэш-функций

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 7.2. Хэш-функции и коллизии

Коллизии и парадокс дней рождения. Практическая демонстрация уязвимостей при некорректной реализации

Текущий контроль
Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет с оценкой, 5 семестр.

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

Промежуточная аттестация: Экзамен, 6 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Введение в криптографию. Основные понятия и определения

Контролируемые ИДК: ОПК-9.1

Тема 1.1. Криптоанализ шифра Виженера

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что изучает криптография?
 1. Методы защиты информации путём её преобразования
 2. Методы сжатия данных
 3. Методы маршрутизации
 4. Методы хранения
2. Основная цель криптографии — обеспечить:
 1. Быструю передачу данных
 2. Конфиденциальность, целостность и подлинность
 3. Архивирование данных
 4. Сжатие файлов
3. Шифр Виженера относится к:
 1. Поточным шифрам
 2. Полиалфавитным шифрам
 3. Блочным шифрам
 4. Асимметричным алгоритмам
4. Метод Касиски применяется для:
 1. Определения длины ключа
 2. Факторизации
 3. Генерации ключа
 4. Подписи
5. Абсолютная стойкость достигается при:
 1. Коротком ключе
 2. Повторном использовании ключа
 3. Одноразовом ключе длиной с сообщение
 4. Использовании MAC

Тема 1.2. Криптоанализ шифра Вернама при условии неоднократного использования одинакового ключа

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Повторное использование ключа в шифре Вернама приводит к:
 1. Увеличению скорости
 2. Потере стойкости
 3. Повышению стойкости
 4. Сжатию данных
2. Какой алгоритм является асимметричным?
 1. AES
 2. DES
 3. RSA
 4. RC4
3. Длина ключа напрямую влияет на:
 1. Цвет интерфейса
 2. Криптостойкость
 3. Размер блока
 4. Формат файла
4. Какое из перечисленных свойств относится к конфиденциальности?
 1. Защита от изменения данных
 2. Защита от несанкционированного раскрытия
 3. Подтверждение личности
 4. Неотказуемость

Раздел 2. Математические основы криптографии

Контролируемые ИДК: ОПК-9.1 ОПК-9.2

Тема 2.1. Схема Диффи–Хеллмана

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В основе RSA лежит сложность:
 1. Дискретного логарифма
 2. Факторизации больших чисел
 3. Коллизий
 4. Сжатия
2. Схема Диффи–Хеллмана основана на задаче:
 1. Факторизации
 2. Дискретного логарифмирования
 3. Коллизий
 4. Хэширования
3. RSA является алгоритмом:
 1. Симметричным
 2. Асимметричным
 3. Поточным
 4. Хэширования
4. Если в RSA выбран слишком маленький модуль n , это приводит к:
 1. Усилению безопасности
 2. Ускорению подписи
 3. Уязвимости к факторизации
 4. Увеличению блока

5. Какой элемент является обязательным для корректной работы протокола Диффи–Хеллмана?

1. Простое число p
2. MAC-код
3. Электронная подпись
4. Хэш длиной 256 бит

Тема 2.2. Криптоанализ алгоритма RSA в базовой форме

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Открытый ключ RSA состоит из:

1. (n, e)
2. (n, d)
3. (p, q)
4. (e, d)

2. Стойкость Диффи–Хеллмана зависит от:

1. Длины сообщения
2. Сложности дискретного логарифма
3. Алфавита
4. Сжатия

3. Если в RSA выбраны малые простые числа, то:

1. Повышается стойкость
2. Упрощается факторизация
3. Ускоряется хэширование
4. Увеличивается MAC

4. Если злоумышленник знает открытый ключ RSA, он может:

1. Расшифровать сообщение без закрытого ключа
2. Подписывать документы от имени владельца
3. Проверять электронную подпись
4. Вычислить закрытый ключ мгновенно

5. В асимметричной криптосистеме открытый ключ используется для:

1. Расшифрования сообщения владельцем
2. Подписания сообщения
3. Шифрования сообщения отправителем
4. Генерации IV

Раздел 3. Стойкость криптоалгоритмов

Контролируемые ИДК: ОПК-9.2 ОПК-9.3

Тема 3.1. Атака с выбором открытого текста

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Атака с выбором открытого текста предполагает:

1. Выбор ключа
2. Возможность шифрования выбранных сообщений
3. Доступ к закрытому ключу
4. Перехват канала

2. Атака с выбором зашифрованного текста предполагает:

1. Возможность расшифрования выбранных шифротекстов
2. Доступ к хэшу
3. Подбор пароля
4. Удаление ключа

3. Хэш-функция должна быть:

1. Обратимой
2. Коллизийно-стойкой
3. Линейной
4. Симметричной

4. Какое свойство обеспечивает невозможность восстановления исходного сообщения по хэш-значению?

1. Коллизийная стойкость
2. Односторонность
3. Линейность
4. Симметричность

5. Как называется атака, при которой перебираются все возможные ключи?

1. Дифференциальная
2. Линейная
3. Полный перебор
4. Коллизийная

6. Какое свойство хэш-функции затрудняет подбор другого сообщения с тем же хэшем для заданного сообщения?

1. Быстрота вычисления
2. Вторая предобразная стойкость
3. Симметричность
4. Обратимость

Тема 3.2. Атака с выбором зашифрованного текста

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Коллизия — это:

1. Совпадение ключей
2. Совпадение хэш-значений разных сообщений
3. Ошибка передачи
4. Сбой сети

2. Парадокс дней рождения применяется для оценки:

1. RSA
2. Вероятности коллизий
3. Скорости шифрования
4. Длины ключа

3. Увеличение длины ключа обычно:

1. Уменьшает стойкость
2. Повышает стойкость
3. Не влияет
4. Уменьшает размер блока

4. Какое свойство обеспечивает невозможность нахождения двух сообщений с одинаковым хэшем?

1. Предобразная стойкость
2. Быстрота вычисления
3. Коллизийная стойкость
4. Симметричность

5. Какое свойство лавинного эффекта означает:

1. Незначительное изменение входа не влияет на выход
2. Малое изменение входа вызывает значительное изменение выхода
3. Сообщение уменьшается
4. Ключ повторяется

6. При использовании слабого генератора случайных чисел безопасность системы:

1. Повышается
2. Не изменяется
3. Снижается
4. Удваивается

Раздел 4. Поточные шифры

Контролируемые ИДК: ОПК-9.2

Тема 4.1. Линейные регистры сдвига с обратной связью (LFSR) и их криптоанализ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Поточный шифр обрабатывает данные:

1. Блоками
2. Потокком бит
3. Архивами
4. Подписями

2. Шифр Вернама относится к:

1. Поточным
2. Блочным
3. Хэш-функциям
4. MAC

3. LFSR используется для:

1. Факторизации
2. Генерации псевдослучайной последовательности
3. Подписи
4. Сжатия

4. Линейная сложность последовательности показывает:

1. Размер ключа
2. Минимальную длину регистра
3. Скорость сети
4. Размер блока

5. Основная слабость линейных генераторов — это:

1. Высокая скорость
2. Предсказуемость
3. Большой ключ
4. Сжатие

6. Что используется для генерации псевдослучайной последовательности в потоковых шифрах?

1. LFSR
2. MAC
3. RSA
4. Хэш-функция

7. Если IV повторяется в режиме CTR, это может привести к:

1. Раскрытию XOR двух сообщений
2. Усилению стойкости
3. Уменьшению длины ключа
4. Ускорению алгоритма

Раздел 5. Блочные шифры

Контролируемые ИДК: ОПК-9.2 ОПК-9.3

Тема 5.1. Режимы шифрования блочных шифров

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Блочный шифр обрабатывает:

1. Поток бит
2. Блок фиксированной длины
3. Хэш
4. Подпись

2. Режим ECB характеризуется:

1. Зависимостью блоков
2. Независимым шифрованием блоков
3. Использованием гаммы
4. Подписью

3. Что является основной уязвимостью режима ECB?

1. Медленная работа
2. Необходимость IV
3. Раскрытие структуры данных
4. Большой ключ

4. В режиме CTR значение счётчика должно быть:

1. Постоянным
2. Секретным
3. Уникальным для каждого блока
4. Равным длине ключа

Тема 5.2. Схема CBC-MAC

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Режим CBC использует:

1. XOR с предыдущим блоком
2. Хэширование
3. Подпись
4. Факторизацию

2. CBC-MAC применяется для:

1. Шифрования
2. Аутентификации
3. Архивирования
4. Сжатия

3. Какой режим шифрования обеспечивает одновременно шифрование и аутентификацию?

1. ECB
2. CBC
3. CTR
4. GCM

Тема 5.3. Реализация атаки на CBC-MAC

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Неправильное использование CBC-MAC может привести к:

1. Коллизии ключей
2. Подделке сообщений
3. Потере файла

4. Увеличению скорости

2. В режиме ECB одинаковые блоки открытого текста:

1. Всегда дают разные шифротексты
2. Дают одинаковые шифротексты
3. Удаляются
4. Сжимаются

3. Какой параметр используется в режиме CBC для повышения случайности?

1. Закрытый ключ
2. Инициализирующий вектор
3. Подпись
4. Хэш

Раздел 6. Криптографические протоколы

Контролируемые ИДК: ОПК-9.1

Тема 6.1. Схема идентификации Шнорра

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Схема Шнорра используется для:

1. Шифрования файлов
2. Идентификации
3. Сжатия
4. Архивирования

2. Диффи–Хеллман позволяет:

1. Подписывать документы
2. Вырабатывать общий секрет
3. Сжимать файлы
4. Хэшировать данные

3. Электронная подпись создаётся с использованием:

1. Открытого ключа
2. Закрытого ключа
3. IV
4. MAC

4. Если злоумышленник может подменить открытый ключ при обмене, возникает атака:

1. Линейная
2. Человек посередине
3. Дифференциальная
4. Коллизионная

5. Какое свойство обеспечивает защиту от повторной передачи перехваченного сообщения?

1. Использование сессионных параметров
2. Увеличение длины блока
3. Сжатие данных
4. Использование ECB

6. Какое свойство обеспечивает невозможность отрицания факта подписи?

1. Конфиденциальность
2. Неотказуемость
3. Диффузия
4. Симметрия

Раздел 7. Построение криптографических примитивов

Тема 7.1. Реализация атаки на алгоритм RSA в базовой форме

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Криптографический примитив — это:
 1. Интерфейс
 2. Базовый алгоритм
 3. Файл
 4. Протокол маршрутизации
2. Основное требование к хэш-функции — это:
 1. Обратимость
 2. Односторонность
 3. Симметричность
 4. Архивация
3. Реализация атаки на RSA возможна при:
 1. Больших простых
 2. Малых простых
 3. Длинном ключе
 4. Хэшировании

Тема 7.2. Хэш-функции и коллизии

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Основное назначение MAC-кода:
 1. Обеспечение конфиденциальности
 2. Обеспечение целостности и аутентичности
 3. Сжатие данных
 4. Генерация ключей
2. Если два разных сообщения имеют одинаковый MAC без знания ключа, это означает:
 1. Успешную атаку
 2. Увеличение стойкости
 3. Нормальную работу алгоритма
 4. Увеличение скорости
3. Основное отличие хэш-функции от шифра состоит в том, что хэш-функция:
 1. Использует секретный ключ
 2. Обратима
 3. Не предназначена для восстановления исходных данных
 4. Работает только с блоками 128 бит

8. Оценочные материалы промежуточной аттестации

5 семестр, Зачет с оценкой

Контролируемые ИДК: ОПК-9.1 ОПК-9.2 ОПК-9.3

Вопросы/Задания:

1. Дайте определение криптографии и охарактеризуйте её основные задачи.
2. Сформулируйте принцип Керкгофса и объясните его значение для построения криптосистем.

3. Объясните различия между симметричными и асимметричными криптосистемами.
4. Опишите шифр Виженера и основные методы его криптоанализа.
5. Объясните принцип работы шифра Вернама и условия его абсолютной стойкости.
6. Почему повторное использование ключа в шифре Вернама приводит к уязвимости?
7. Раскройте математические основы алгоритма RSA.
8. Опишите процесс генерации открытого и закрытого ключей в RSA.
9. Объясните, в чём состоит криптостойкость алгоритма RSA.
10. Опишите протокол Диффи–Хеллмана и его математическую основу.
11. В чём заключается атака «человек посередине» при использовании Диффи–Хеллмана?
12. Дайте определение криптографической стойкости алгоритма.
13. Охарактеризуйте модель атаки с выбором открытого текста.
14. Охарактеризуйте модель атаки с выбором зашифрованного текста.
15. Дайте определение хэш-функции и перечислите её основные свойства.
16. Объясните понятие коллизии хэш-функции и парадокс дней рождения.
17. Раскройте понятие лавинного эффекта в криптографических алгоритмах.
18. Объясните принципы построения потоковых шифров.
19. Охарактеризуйте линейные регистры сдвига с обратной связью и их применение.
20. Сравните потоковые и блочные шифры.
21. Опишите структуру блочного шифра.
22. Охарактеризуйте режимы шифрования ECB и CBC и их особенности.
23. Объясните назначение и принципы работы режима CTR.
24. Раскройте назначение и принципы работы схемы CBC-MAC.
25. Объясните различие между шифрованием и аутентификацией сообщений.
26. Дайте определение электронной подписи и опишите её основные свойства.

27. Объясните понятие неотказуемости и его значение в криптографии.
28. Дайте определение криптографического примитива и приведите примеры.
29. Объясните требования к генераторам случайных и псевдослучайных чисел в криптографии.
30. Охарактеризуйте основные угрозы безопасности при некорректной реализации криптографических алгоритмов.

6 семестр, Экзамен

Контролируемые ИДК: ОПК-9.1 ОПК-9.2 ОПК-9.3

Вопросы/Задания:

1. Классификация криптосистем и их сравнительная характеристика.
2. Принцип Керкгофса и его значение при проектировании криптографических систем.
3. Математические основы современной криптографии: арифметика по модулю и её применение.
4. Теоретические основы абсолютной стойкости шифров. Теорема Шеннона.
5. Криптоанализ классических полиалфавитных шифров на примере шифра Виженера.
6. Шифр Вернама и условия обеспечения его абсолютной стойкости.
7. Линейные регистры сдвига с обратной связью: принципы построения и анализ стойкости.
8. Поточные шифры: принципы работы, преимущества и недостатки.
9. Блочные шифры: структура, принципы конфузии и диффузии.
10. Режимы работы блочных шифров: сравнительный анализ ECB, CBC, CTR, GCM.
11. Назначение и принципы работы схемы CBC-MAC. Анализ возможных уязвимостей.
12. Криптографические хэш-функции: требования и свойства.
13. Коллизии хэш-функций и методы оценки вероятности их возникновения.
14. Лавинный эффект и его значение для криптостойкости алгоритмов.
15. Модели криптоаналитических атак: атака с известным открытым текстом, с выбором открытого текста и с выбором шифротекста.
16. Полный перебор ключей (brute-force) и факторы, влияющие на его сложность.

17. Алгоритм RSA: математические основы, генерация ключей и принципы работы.
18. Уязвимости алгоритма RSA при неправильном выборе параметров.
19. Протокол Диффи–Хеллмана: принципы построения и анализ безопасности.
20. Атака «человек посередине» и методы её предотвращения.
21. Электронная подпись: назначение, свойства и алгоритмическая реализация.
22. Схема идентификации Шнорра: принципы построения и анализ стойкости.
23. Понятие криптографического примитива и его роль в построении протоколов.
24. Требования к генераторам случайных и псевдослучайных чисел в криптографии.
25. Понятие сессионного ключа и его применение в протоколах защищённого обмена.
26. Механизмы обеспечения целостности и аутентичности сообщений.
27. Сравнительный анализ симметричных и асимметричных методов защиты информации.
28. Основные угрозы безопасности при реализации криптографических алгоритмов.
29. Аппаратные и программные средства криптографической защиты информации.
30. Современные направления развития криптографии и перспективные методы защиты информации.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Жиль Земор Курс криптографии / Земор Жиль; перевод В. В. Шуликовская. - Курс криптографии - Москва, Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019. - 256 с. - 978-5-4344-0770-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/91941.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Введение в теоретико-числовые методы криптографии / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург: Лань, 2022. - 400 с. - 978-5-8114-1116-0. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/210746.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке
3. Басалова Г. В. Основы криптографии: учебное пособие: учебное пособие / Г. В. Басалова. - Основы криптографии - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 282 с. - 978-5-4497-2420-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/133959.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Сергиенко Е. Н. Математические методы кодирования и шифрования: учебное пособие: учебное пособие / Е. Н. Сергиенко. - Математические методы кодирования и шифрования - Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ, 2017. - 101 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/92262.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Криптоалгоритм «Люцифер». Основы теории современного шифрования: научное издание: научное издание / К. Д. Ермаков, Ю. В. Кузнецов, А. П. Мартынов, Д. Б. Николаев, М. В. Одинцов. - Криптоалгоритм «Люцифер». Основы теории современного шифрования - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2022. - 137 с. - 978-5-9515-0504-0. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/132630.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Никифоров С. Н. Методы защиты информации. Шифрование данных: учебное пособие: учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург: Лань, 2022. - 160 с. - 978-5-8114-4042-9. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/206285.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие для вузов: учебное пособие для вузов / С. Н. Никифоров. - 5-е изд., стер. - Санкт-Петербург: Лань, 2023. - 124 с. - 978-5-507-47181-2. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/338018.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"
2. <http://citforum.ru> - IT-портал CITForum
3. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
4. <https://www.elibrary.ru/> - НЭБ eLIBRARY

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.
Моноблок - 64 шт.
Проектор - 4 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.
Доска настенная одноэлементная - 2 шт.
Интерактивная панель - 1 шт.
Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.