МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Методы и средства криптографической защиты информации
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Доцент, к.ф.-м.н.
Тюлюкин В.А.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование у студентов теоретических знаний по принципам защиты информации с помощью криптографических методов и реализации этих методов на практике. Содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, основными алгоритмами шифрования и криптографическими протоколами обмена информацией

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Практические занятия, включая курсовое проектирование		
Семестр 6						
Экзамен	144	64	32	32	53	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ИД-1.ОПК-3 Знать: основы линейной алгебры, основные понятия и задачи векторной алгебры и аналитической геометрии, основные положения теории пределов функций, теории рядов, основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных, основные понятия и методы теории вероятностей, математической статистики, основные понятия и методы дискретной математики
	ИД-2.ОПК-3 Уметь: использовать для решения прикладных задач соответствующий математический аппарат

ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ИД-3.ОПК-3 Владеть: навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач, навыками решения задач линейной алгебры и аналитической геометрии, навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач, навыками решения оптимизационных задач с использованием средств вычислительной техники
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ИД-1.ОПК-9 Знать: основные положения практики криптографической и технической защиты информации; основные проектные решения, средства и методы криптографической защиты информации, технические средства защиты информации
	ИД-2.ОПК-9 Уметь: решать типовые задачи с помощью методов криптологии, устанавливать, настраивать и обслуживать технические средства защиты информации
	ИД-3.ОПК-9 Владеть: навыками эксплуатации криптографических протоколов и схем, навыками применения средств технической защиты информации для решения задач профессиональной деятельности

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		117					
Тема 1.	История развития криптографии. Основные понятия (ОПК-3)	2	2				
Тема 2.	Математические основы криптографии. Надежность шифров. Основы теории К. Шеннона. Хеш-функции (ОПК-9)	19	4		2	13	
Тема 3.	Введение в криптографические методы защиты информации (ОПК-3)	34	4		14	16	
Тема 4.	Системы симметричного и асимметричного шифрования (ОПК-9)	44	16		12	16	
Тема 5.	Электронная цифровая подпись. Открытое распространение ключей	18	6		4	8	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания

Текущий контроль (Приложение 4)			
Тема 1. История развития криптографии. Основные понятия	Тест (Приложение 4)	Примерный перечень вопросов теста	100 баллов
Тема 2. Математические основы криптографии. Надежность шифров. Основы теории К. Шеннона. Хеш-функции	Контрольная работа №1 (Приложение 4)	Контрольная работа состоит из 8 практических заданий в 1 части и 6 практических заданий 2 части.	20 баллов
Тема 3. Введение в криптографические методы защиты информации	Контрольная работа №2 (Приложение 4)	Контрольная работа состоит из 16 вариантов по 1 практическому заданию.	20 баллов
Тема 4. Системы симметричного и асимметричного шифрования	Контрольная работа №3 (Приложение 4)	Контрольная работа состоит из 3 практических заданий.	20 баллов
Тема 5. Электронная цифровая подпись. Открытое распространение ключей	Контрольная работа №4 (Приложение 4)	Контрольная работа состоит из 5 практических заданий.	20 баллов
Промежуточная аттестация(Приложение 5)			
6 семестр (Эк)	Экзаменационный билеты (Приложение 5)	В каждом билете 2 вопроса теоретических и 1 практический	100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. История развития криптографии. Основные понятия (ОПК-3)
Основные понятия криптографии. Стойкость шифров. Теоретическая и практическая стойкость криптосистем. Обобщенная схема для криптосистем с закрытыми ключами шифрования. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации.
Основы криптоанализа. История создания частотного анализа. Одноалфавитный шифр. Многоалфавитные шифры. Омофонический шифр замены. Диграф. Великий шифр. Шифр Билля. Шифр Виженера. Взлом шифра Виженера.

Тема 2. Математические основы криптографии. Надежность шифров. Основы теории К. Шеннона. Хеш-функции (ОПК-9)
Понятие вычета по модулю. Понятие сравнимости двух чисел. Введение в конечные поля. Понятие группы. Операции в группах. Кольцо. Поле. Поле Галуа. Неприводимые многочлены. Простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Мультипликативность функции. Китайская теорема об остатках. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Алгоритм Евклида. Расширенный алгоритм Евклида. Показатели и первообразные корни. Дискретные логарифмы. Генераторы случайных чисел. Проверка качества работы ГСЧ. Преобразование Уолша-Адамара. Эллиптические кривые. Тесты числа на простоту. Принципы построения больших простых чисел. Алгоритм Адлемана-Ленстры. Разложение составных чисел на множители.
Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. «Ненадёжность шифра» и «расстояние единственности». Практически стойкие шифры.
Понятие хеш-функции. Коллизия. Хеш-функции Наорра и Юнга. Проверка целостности информации с использованием хеш-функций. Нахождение коллизий хеш-функций в общем случае. Парадокс о днях рождения. Атака «встреча посередине» для хеш-функций. Линейное разделение секрета.

Тема 3. Введение в криптографические методы защиты информации (ОПК-3)
Особенности криптографических методов защиты информации. Криптология, криптография и криптоанализ. Шифромашины. Основные понятия криптографии: шифра, алгоритма шифрования, ключа шифрования, криптосистемы. Атаки на шифр. Правило Керкхоффа. Стойкость шифра. Зависимость криптографии от уровня технологий

Тема 4. Системы симметричного и асимметричного шифрования (ОПК-9)
Простейшие шифры и их свойства, шифры замены и перестановки, композиции шифров. Блочные и поточные (потоковые) шифры. Алгоритмы шифрования на основе сетей Фейстеля. Стандарты шифрования данных DES, AES и ГОСТ 28147-89. Режимы работы блочных шифров. Алгоритмы Lucifer, IDEA, Blowfish. Потоковые шифры A5 и RC4.
Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией. Криптосистема RSA.
Криптографические протоколы. Проблемы криптографических протоколов. Последние достижения в криптоанализе

Тема 5. Электронная цифровая подпись. Открытое распространение ключей
Электронная цифровая подпись: требования к цифровой подписи, стандарт DSS, прямая цифровая подпись, технологии арбитражной цифровой подписи. Криптографические функции хеширования. Отечественные стандарты криптографической защиты информации ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ Р34.10-2001. Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509).

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Математические основы криптографии. Надежность шифров. Основы теории К. Шеннона. Хеш-функции (ОПК-9) Проверка целостности информации с использованием хеш-функций. Нахождение коллизий хеш-функций в общем случае. Парадокс о днях рождения. Атака «встреча посередине» для хеш-функций. Линейное разделение секрета
Тема 3. Введение в криптографические методы защиты информации (ОПК-3) Особенности криптографических методов защиты информации. Криптология, криптография и криптоанализ. Шифромашины. Основные понятия криптографии: шифра, алгоритма шифрования, ключа шифрования, криптосистемы. Атаки на шифр. Правило Керкхоффа. Стойкость шифра. Зависимость криптографии от уровня технологий
Тема 4. Системы симметричного и асимметричного шифрования (ОПК-9) Простейшие шифры и их свойства, шифры замены и перестановки, композиции шифров. Блочные и поточные (потоковые) шифры. Алгоритмы шифрования на основе сетей Фейстеля. Стандарты шифрования данных DES, AES и ГОСТ 28147-89. Режимы работы блочных шифров. Алгоритмы Lucifer, IDEA, Blowfish. Потоковые шифры A5 и RC4. Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией. Криптосистема RSA. Криптографические протоколы. Проблемы криптографических протоколов. Последние достижения в криптоанализе
Тема 5. Электронная цифровая подпись. Открытое распространение ключей Электронная цифровая подпись: требования к цифровой подписи, стандарт DSS, прямая цифровая подпись, технологии арбитражной цифровой подписи. Криптографические функции хеширования. Отечественные стандарты криптографической защиты информации ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ Р34.10-2001. Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509).

7.3. Содержание самостоятельной работы

Тема 3. Введение в криптографические методы защиты информации (ОПК-3) Домашняя контрольная работа
Тема 4. Системы симметричного и асимметричного шифрования (ОПК-9) домашняя контрольная работа
Тема 5. Электронная цифровая подпись. Открытое распространение ключей тест

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Романьков В. А. Введение в криптографию [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2021. - 240 – Режим доступа: https://znanium.com/catalog/product/1514566

Дополнительная литература:

2. Кнауб Л.В., Новиков Е.А., Шитов Ю. А. Теоретико-численные методы в криптографии [Электронный ресурс]:Учебное пособие. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. – Режим доступа: https://znanium.com/catalog/product/441493

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Microsoft Visual Studio Community. Лицензия для образовательных учреждений. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

Интернет-университет информационных технологий
http://www.intuit.ru

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

К экзамену

I. Математические основы криптографии

1. Основные понятия криптографии: шифр, алгоритм шифрования, ключ шифрования, криптосистема. Обобщенная схема для криптосистем с закрытыми ключами шифрования.
2. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Криптология, криптография и криптоанализ.
3. Основы криптоанализа. Определение. История создания частотного анализа. Попытки совершенствования одноалфавитного шифра.
4. Многоалфавитные шифры. Омофонический шифр замены. Диграф. Великий шифр. Шифр Билля.
5. Шифр Виженера. Беббидж и его роль во взломе шифра Виженера. Взлом шифра Виженера
6. Понятие вычета по модулю. Понятие сравнимости двух чисел.
7. Введение в конечные поля. Понятие группы. Циклическая группа. Правила выполнения операций в группах.
8. Кольцо. Кольцо с единицей. Подкольцо. Целостное кольцо.
9. Поле. Порядок и степень поля. Поле Галуа. Примитивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.
10. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о существовании обратного числа.
11. Мультипликативность функции.
12. Теорема Ферма.
13. Функция Эйлера. Функция Мебиуса
14. Теорема Эйлера.
15. Алгоритм Евклида. Расширенный алгоритм Евклида.
16. Показатели и первообразные корни.
17. Генераторы случайных чисел. Методы построения ГСЧ.
18. Проверка качества работы ГСЧ. Проверка на равномерность распределения. Проверка на статистическую независимость.
19. Преобразование Уолша-Адамара. Функции Уолша.
20. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.
21. Тесты числа на простоту. Принципы построения больших простых чисел.
22. Алгоритм Адлемана-Ленстры.
23. Разложение составных чисел на множители.
24. Дискретные логарифмы.
25. Понятие хеш-функции. Коллизия. Хеш-функции Наорра и Юнга.
26. Проверка целостности информации с использованием хеш-функций.
27. Построение хеш-функции на основе блочных преобразований.
28. Нахождение коллизий хеш-функций в общем случае. Парадокс о днях рождения.
29. Атака «встреча посередине» для блочных хеш-функций.
30. Линейное разделение секрета.
31. Стойкость шифров. Правило Керкхоффа. Теоретическая и практическая стойкость криптосистем.
32. Математические основы криптографии. Теоретическая и практическая стойкость

криптосистем. Теорема Шенона о совершенной секретности.

33. Математические основы криптографии. Ненадежность шифров и расстояние единственности.

II. Основы прикладной криптографии

1. Понятие блочного и поточного шифра. Алгоритмы шифрования на основе сетей Фейстеля.
2. Стандарт шифрования данных DES. Основные характеристики.
3. Обобщенная схема шифрования в алгоритме DES. Операции начальной и конечной перестановок.
4. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операции расширения и перестановки бит.
5. Схема вычисления функции шифрования для одного раунда алгоритма DES. Операция преобразования на S-блоках.
6. Схема вычисления раундовых ключей в алгоритме DES.
7. Режимы работы блочных шифров. Комбинирование блочных шифров. Криптосистема 3DES.
8. Стандарт шифрования ГОСТ 28147-89. Основные характеристики.
9. Стандарт шифрования AES. Основные характеристики.
10. Потоковые шифры A5 и RC4. Основные характеристики.
11. Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
12. Криптосистема RSA.
13. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
14. Электронная цифровая подпись. Свойства электронной цифровой подписи. Стандарт DSS. Схема генерации и проверки электронной цифровой подписи.
15. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования. Алгоритм хеширования SHA.
16. Стандарты электронной цифровой подписи ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и функции хеширования ГОСТ Р 34.11-94. Основные характеристики.
17. Открытое распространение ключей. Инфраструктура открытого распространения ключей и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509).
18. Системы электронной безопасности в финансовой сфере. Аутентификация данных на картах. Статическая и динамическая аутентификация.
19. Системы электронной безопасности в финансовой сфере. Системы аутентификации смарт-карт и терминалов на базе симметричных криптосистем.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

ЗАДАНИЯ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ
10.03.01 Информационная безопасность
Дисциплина: Методы и средства криптографической защиты информации

Компетенция ОПК-3; ОПК-9

ОПК-3 Способен использовать необходимые математические методы для решения задач профессиональной деятельности;

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

Задания закрытого типа

1. Что такое криптография?

a) Наука о скрытии информации от посторонних глаз

b) Наука о компьютерной безопасности

c) Наука о создании криптовалют

d) Наука о хранении информации в облаке

Ответ: A

2. Какой тип атаки на шифр Цезаря позволяет расшифровать сообщение без знания ключа?

a) Атака методом перебора

b) Атака методом подбора

c) Атака методом погружения

d) Атака методом линейной аппроксимации

Ответ: A

3. Какой из следующих алгоритмов является симметричным шифром?

a) RSA

b) AES

c) Diffie-Hellman

d) ElGamal

Ответ: B

4. Что такое публичный ключ в криптографии?

a) Секретный ключ, который используется для расшифровки сообщений

b) Открытый ключ, который используется для шифрования сообщений

c) Секретный ключ, который используется для шифрования сообщений

d) Открытый ключ, который используется для расшифровки сообщений

Ответ: B

5. Что такое хеш-функция в криптографии?

a) Алгоритм шифрования, который использует секретный ключ

b) Алгоритм шифрования, который использует открытый ключ

c) Алгоритм, который преобразует произвольный вход в фиксированный выход

d) Алгоритм, который преобразует фиксированный вход в произвольный выход

Ответ: C

6. Какой алгоритм используется для создания цифровой подписи?

a) RSA

b) AES

c) SHA-256

d) MD5

Ответ: A

7. Что такое атака "человек посередине" (man-in-the-middle)?

a) Атака, при которой злоумышленник перехватывает и изменяет передаваемые данные

b) Атака, при которой злоумышленник подделывает свой IP-адрес

c) Атака, при которой злоумышленник выдает себя за другого пользователя

d) Атака, при которой злоумышленник взламывает сервер

Ответ: A

8. Какой из следующих алгоритмов шифрования использует симметричное шифрование?

a) RSA

b) AES

c) ECC

d) Diffie-Hellman

Правильный ответ: b) AES

9. Что такое открытый ключ в криптографии?

a) Секретный ключ для шифрования данных

b) Пара ключей, используемая для шифрования и дешифрования данных

c) Ключ для вычисления цифровой подписи

d) Ключ для аутентификации пользователя

Правильный ответ: b) Пара ключей, используемая для шифрования и дешифрования данных

10. Какой алгоритм шифрования считается наиболее надежным на сегодняшний день?

a) DES

b) Triple DES

c) AES

d) RC4

Правильный ответ: c) AES

Задания открытого типа

1. Что такое криптография? Приведите пример.
2. Какие типы криптографии существуют? Приведите пример.

3. Какой метод криптографии является наиболее безопасным? Приведите пример.
4. Как работают симметричные алгоритмы шифрования? Приведите пример.
5. Как работают асимметричные алгоритмы шифрования? Приведите пример.
6. Что такое ключ шифрования? Приведите пример.
7. Какие методы атаки могут быть использованы для взлома шифрования? Приведите пример.
8. Какой алгоритм шифрования используется в SSL/TLS? Приведите пример.
9. Что такое цифровая подпись? Приведите пример.
10. Как работает протокол Диффи-Хеллмана? Приведите пример.
11. Что такое атака "человек посередине" (man-in-the-middle)? Приведите пример.
12. Как работает атака "отказ в обслуживании" (DDoS)? Приведите пример.
13. Какие типы сертификатов SSL/TLS существуют? Приведите пример.
14. Как работает атака "словарь" (dictionary attack)? Приведите пример.
15. Как работает атака "брутфорс" (brute force)? Приведите пример.
16. Как работает атака "фишинг" (phishing)? Приведите пример.
17. Как работает атака "внедрение SQL-кода" (SQL injection)? Приведите пример.
18. Как работает атака "межсайтовое выполнение сценариев" (cross-site scripting)? Приведите пример.
19. Как работает атака "межсайтовая подделка запроса" (cross-site request forgery)? Приведите пример.
20. Как работает атака "бэкдор" (backdoor)? Приведите пример.
21. Как работает атака "компрометация сети" (network compromise)? Приведите пример.
22. Как работает атака "внедрение вредоносного кода" (malware injection)? Приведите пример.
23. Как работает атака "мануальная установка" (manual installation)? Приведите пример.
24. Конечно, вот 35 простых вопросов к зачету по криптографии, с просьбой привести пример в конце каждого вопроса:
25. Что такое криптография? Приведите пример.
26. Каковы основные цели криптографии? Приведите пример.
27. Что такое симметричное шифрование? Приведите пример.
28. Что такое асимметричное шифрование? Приведите пример.
29. Что такое хэш-функция? Приведите пример.
30. Каковы основные свойства хорошей хэш-функции? Приведите пример.