УТВЕРЖДЕНО

решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Методы и средства криптографической защиты информации**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Рацеев Сергей Михайлович	Кафедра информационной безопасности и теории управления	Профессор,Доктор физико-математических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-3, ОПК-9.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Теория кодирования, сжатия и восстановления информации, Методы и средства криптографической защиты информации, Теория псевдослучайных генераторов, Вычислительные методы в алгебре и теории чисел, Математическая логика и теория алгоритмов, Дифференциальные уравнения, Алгебра и геометрия, Теория вероятностей, Математический анализ, Научно-исследовательская работа, Численные методы, Ознакомительная практика, Методы алгебраической геометрии в криптографии, Избранные вопросы математического анализа, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Разработка и эксплуатация автоматизированных систем в защищенном исполнении, Защита информации от утечки по техническим каналам.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	**знать**: алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	логарифмирования в конечных циклических группах **уметь**: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ **владеть**: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;	**знать**: основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; основные виды симметричных и асимметричных криптографических алгоритмов; **уметь**: корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; **владеть**: криптографической терминологией; навыками использования типовых криптографических алгоритмов;

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 7 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 252 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)		
	Всего по плану	В т.ч. по семестрам	
		7	8
1	2	3	4
Контактная работа обучающихся с преподавателем в соответствии с УП	144	72	72
Аудиторные занятия:	144	72	72
Лекции	72	36	36
Семинары и практические занятия	-	0	0
Лабораторные работы, практикумы	72	36	36
Самостоятельная работа	72	36	36

Вид учебной работы	Количество часов (форма обучения очная)		
	Всего по плану	В т.ч. по семестрам	
		7	8
1	2	3	4
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование	
Курсовая работа	-	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет, Экзамен (24)	Зачет	Экзамен
Всего часов по дисциплине	252	108	144

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Надежность шифров							
Тема 1.1. Шифры замены и перестановки	18	8	0	2	2	8	Вопросы к Экзамену, Тестирование
Тема 1.2. Совершенные шифры.	52	24	0	4	4	24	Вопросы к Экзамену, Тестирование
Раздел 2. Схемы разделения секрета							
Тема 2.1. Пороговые схемы разделения секрета.	12	4	0	4	4	4	Вопросы к Экзамену, Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 2.2. Схемы разделения секрета с произвольной структурой доступа.	8	4	0	0	0	4	Вопросы к Экзамену, Тестирование
Раздел 3. Блочные шифры и электронные подписи							
Тема 3.1. Симметричные блочные шифры	20	4	0	12	2	4	Вопросы к Экзамену, Тестирование
Тема 3.2. Шифрование с открытым ключом	20	4	0	12	0	4	Вопросы к Экзамену, Тестирование
Тема 3.3. Электронная подпись	22	8	0	6	0	8	Вопросы к Экзамену, Тестирование
Раздел 4. Протоколы аутентификации и передачи ключей							
Тема 4.1. Протоколы аутентификации	32	8	0	16	0	8	Вопросы к Экзамену, Тестирование
Тема 4.2. Протоколы с нулевым разглашением	24	4	0	16	0	4	Вопросы к Экзамену, Тестирование
Тема 4.3. Протоколы передачи ключей	8	4	0	0	0	4	Вопросы к Экзамену, Тестирование
Итого подлежит изучению	216	72	0	72	12	72	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Надежность шифров

Тема 1.1. Шифры замены и перестановки

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров. Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе проверки гипотезы с использованием леммы Неймана-Пирсона. Критерий на основе запретных m-грамм.

Тема 1.2. Совершенные шифры.

Формальные модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра. Математические модели некоторых шифров. Математическая модель шифра простой замены. Математическая модель шифра сдвига. Математическая модель шифра перестановки. Математическая модель аффинного шифра. Математическая модель шифра Хилла. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. Примеры совершенных шифров. (k|y)-совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия (k|y)-совершенных шифров. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров. Примеры (k|y)-совершенных шифров. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей. Подмена шифрованного сообщения. Имитация шифрованного сообщения. Имитостойкость шифра. Нижние оценки вероятности имитации и подмены сообщения. Примеры совершенных имитостойких шифров. Шифры, не распространяющие искажений типа замены знаков. Метрика Хэмминга на открытых и шифрованных текстах. Определение шифра, не распространяющего искажений типа замены знаков. Эквивалентные условия шифра, не распространяющего искажений типа замены знаков. Понятие изометрии. Теорема А.А.Маркова. Шифры, не распространяющие искажений типа пропуска

(вставки) знаков. Определение шифра, не распространяющего искажений типа пропуска знаков. Эквивалентные условия шифра, не распространяющего искажений типа пропуска знаков. Критерий шифра, не распространяющего искажений типа пропуска знаков, в классе эндоморфных шифров.

Раздел 2. Схемы разделения секрета

Тема 2.1. Пороговые схемы разделения секрета.

Аддитивная схема разделения секрета. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схема разделения секрета Блэкли. Реплицированная схема разделения секрета. Схема Миньотта. Схема Асмута—Блума.

Тема 2.2. Схемы разделения секрета с произвольной структурой доступа.

Структуры доступа, связанные с разбиением множества участников. Схема Ито-Саито-Нишизеки. Схемы для конъюнктивных иерархических структур доступа. Схемы для дизъюнктивных иерархических структур доступа.

Раздел 3. Блочные шифры и электронные подписи

Тема 3.1. Симметричные блочные шифры

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Режимы использования блочных шифров. Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES.

Тема 3.2. Шифрование с открытым ключом

Задачи, приводящие к криптографии с открытым ключом. Понятие односторонней функции. Быстрое (бинарное) возведение в степень. Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамаля. Ограничения на параметры системы. Модификация шифра Эль-Гамаля на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей.

Тема 3.3. Электронная подпись

Определение хеш-функции. Примеры хеш-функций. Целесообразность использования хеш-

функций. Основные требования, которым должна удовлетворять хеш-функция. Зависимость данных требований друг от друга. Парадокс дней рождений. Построение хеш-функций. Примеры криптографических хеш-функций. Коды аутентификации. Основные понятия. Имитация и подмена для кода аутентификации. Нижние границы вероятностей имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации. Ортогональные таблицы. Математическая модель кода аутентификации с неограниченным ключом. Примеры оптимальных кодов аутентификации с неограниченным ключом. Задачи, решаемые с помощью электронных подписей. Надежность электронной подписи. Электронная подпись на основе шифрсистем с открытыми ключами. Электронные подписи на основе симметричных криптосистем. Примеры электронных подписей. Подпись Фиата-Шамира. Подпись Эль-Гамаля. Подпись RSA. Подпись Шнорра. Одноразовые электронные подписи.

Раздел 4. Протоколы аутентификации и передачи ключей

Тема 4.1. Протоколы аутентификации

Протоколы аутентификации, использующие пароли (слабая аутентификация). Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования. Протокол аутентификации Фиата-Шамира. Протокол Фейга-Фиата-Шамира. Итеративный протокол аутентификации Фиата-Шамира без доверенного центра. Трехпроходный протокол аутентификации Фиата-Шамира без доверенного центра. Протокол аутентификации Шнорра. Итеративный и трехпроходный модифицированный протокол Шнорра. Модификация протокола Шнорра на эллиптических кривых. Итеративный и трехпроходный модифицированный протокол Шнорра на эллиптических кривых. Протокол аутентификации Окамото. Модификация протокола Окамото на эллиптических кривых. Протокол аутентификации Гиллоу-Куискатр (GQ). Протокол аутентификации с нулевым разглашением на основе доказательства изоморфизма графов. Пятипроходный протокол аутентификации на основе изоморфизма графов с использованием эллиптических кривых. Протокол аутентификации с нулевым разглашением на основе асимметричных шифров. Протокола аутентификации с нулевым разглашением на основе шифра RSA. Протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.

Тема 4.2. Протоколы с нулевым разглашением

Протокол подбрасывания монеты по телефону. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Протоколы привязки к биту. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.

Тема 4.3. Протоколы передачи ключей

Передача ключей с использованием симметричного шифрования: двусторонние протоколы. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы.

Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протоколы MTI. Модификация семейства протоколов MTI на эллиптических кривых. Предварительное распределение ключей. Схема Блома.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Шифры замены и перестановки
Цели: Разработать криптографическую защиту информации, содержащейся в текстовом (двоичном) файле данных, с помощью алгоритма шифрования, указанного в варианте.
Содержание: 1. Разработать алгоритмы шифрования и расшифрования открытого текста из алфавита A на заданном ключе с помощью метода, указанного в варианте. 2. Определить алфавит A криптосистемы (открытого текста и шифртекста). Если алфавит A не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. 3. Написать функцию генерации случайных ключей шифра, оценить размерность ключевого пространства. 4. Написать функцию, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами. 5. Написать функцию для реализации алгоритма расшифрования полученного шифрованного файла при известном ключе.
Результаты: Основное внимание должно быть уделено освоению классических шифров.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Российский стандарт симметричного шифрования ГОСТ Р 34.12-2015
Цели: Ознакомиться с шифрованием и расшифрованием информации при помощи алгоритма “Магма” из ГОСТ Р 34.12-2015.
Содержание: Реализовать шифр “Магма” из ГОСТ Р 34.12-2015 и основные режимы шифрования.
Результаты: Основное внимание должно быть уделено освоению шифра “Магма” из ГОСТ Р 34.12-2015 и основных режимов шифрования.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Схемы разделения секрета
Цели: Изучение пороговых схем разделения секрета.
Содержание: Реализовать схему разделения секрета в соответствии с индивидуальным вариантом. Программа должна уметь как разделять секрет на участников в соответствии с порогом , так и восстанавливать его. Варианты заданий: 1. Схема разделения секрета Шамира. 2. Схема разделения секрета на основе равновесных двоичных кодов. 3. Схема разделения секрета на основе китайской теоремы об остатках.
Результаты: Основное внимание должно быть уделено освоению принципов построения схем разделения секрета.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Асимметричные шифры
Цели: Освоить методику работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для расшифрования.
Содержание: Требуется реализовать программу, работающую по алгоритму Эль-Гамаля. Программа

должна уметь работать с текстом произвольной длины.
Результаты: Основное внимание должно быть уделено освоению ассиметричных шифров.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Электронная подпись
Цели: Освоить методику работы электронных подписей.
Содержание: Требуется реализовать электронную подпись Эль-Гамаля.
Результаты: Основное внимание должно быть уделено освоению алгоритмов электронных подписей.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Протоколы аутентификации
Цели: Освоить методику работы протоколов аутентификации.
Содержание: Требуется реализовать протокол аутентификации Фиата-Шамира.
Результаты: основное внимание должно быть уделено освоению протоколов аутентификации.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Протоколы с нулевым разглашением
Цели: Изучение протоколов привязки к биту.
Содержание: Реализовать протокол привязки к биту на основе протокола Шнорра.
Результаты: Основное внимание должно быть уделено освоению протоколов привязки к биту.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ, ЗАЧЕТУ

Вопросы к экзамену

1. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига, аффинный шифр.
2. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.
3. Многоалфавитные шифры замены: аффинный блочный шифр.
4. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.
5. Алгебраическая и вероятностная модели шифров.
6. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.
7. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.
8. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.
9. (k|y)-совершенные шифры: определение, эквивалентные условия.
10. Необходимые и достаточные условия (k|y)-совершенных шифров.
11. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров.
12. Аддитивная схема разделения секрета.
13. Схема разделения секрета Шамира.
14. Проверяемая схема разделения секрета Фельдмана-Шамира.

15. Совершенная проверяемая схема разделения секрета Педерсона-Шамира.
16. Схема разделения секрета Блэкли.
17. Реплицированная схема разделения секрета.
18. Схема Миньотта. Схема Асмута—Блума.
19. Структуры доступа, связанные с разбиением множества участников.
20. Схема Ито-Саито-Нишизеки.
21. Схемы для конъюнктивных иерархических структур доступа.
22. Схемы для дизъюнктивных иерархических структур доступа.
23. Итеративные блочные шифры. Обратимость итеративного блочного шифра.
24. Шифры Фейстеля и их обратимость.
25. Режимы использования симметричных блочных шифров.
26. Шифр Магма из ГОСТ Р 34.12-2015.
27. Алгоритм быстрого возведения в степень. Первообразные корни. Схема Диффи-Хеллмана.
28. Криптосистема Месси-Омуры. Вероятностный шифр Эль-Гамаля.
29. Шифр RSA. Рюкзачные криптосистемы, система Меркла-Хеллмана.
30. Хеш-функции. Требования, предъявляемые к хеш-функциям.
31. Криптографические хеш-функции. Способы построения криптографических хеш-функций.
32. Хеш функция из ГОСТ 34.11.2012.
33. Определение электронной подписи, основные свойства. Электронная подпись RSA.
34. Электронная подпись Фиата-Шамира, Эль-Гамаля, Шнорра.
35. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования.
36. Протоколы аутентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования и электронной подписи.
37. Протокол аутентификации Фиата-Шамира.
38. Протокол Фейга-Фиата-Шамира.
39. Протокол аутентификации Шнорра.
40. Протокол подбрасывания монеты по телефону. Протокол на основе хеш-функции.
41. Протоколы привязки к биту. Протокол привязки к биту на основе протокола Шнорра.
42. Передача ключей с использованием симметричного шифрования: двусторонние протоколы.
43. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos.
44. Передача ключей с использованием асимметричного шифрования.
45. Открытое распределение ключей. Протокол MTI.

Вопросы к зачету

1. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.

2. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.

3. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.

4. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.

5. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.

6. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).

7. Алгебраическая и вероятностная модели шифров.

8. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр.

9. Детерминированная модель открытого текста.

10. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

11. Математическая модель некоторых шифров: шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

12. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.

13. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.

14. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.

15. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей.

16. Примеры совершенных шифров с условиями $|X|=|Y|=|K|$, $|X|<|Y|=|K|$, $|X|=|Y|<|K|$, $|X|<|Y|<|K|$.

17. (k|y)-совершенные шифры: определение, эквивалентные условия.

18. Необходимые и достаточные условия (k|y)-совершенных шифров.

19. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров.

20. Примеры (k|y)-совершенных шифров с условиями $|X|=|Y|>|K|$, $|X|=|Y|=|K|$, $|X|=|Y|<|K|$.

21. Примеры одновременно совершенного и (k|y)-совершенного шифра с условиями $|X|=|Y|=|K|$,

|X|=|Y|<|K|.

22. Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ.

23. Схема разделения секрета Шамира.

24. Проверяемая схема разделения секрета Фельдмана-Шамира.

25. Совершенная проверяемая схема разделения секрета Педерсона-Шамира.

26. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

27. Схема разделения секрета на основе китайской теоремы об остатках.

28. Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера.

29. Схема Ито-Саито-Нишизеки.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Надежность шифров			
Тема 1.1. Шифры замены и перестановки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 1.2. Совершенные шифры.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	24	Тестирование
Раздел 2. Схемы разделения секрета			
Тема 2.1. Пороговые схемы разделения секрета.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.2. Схемы разделения секрета с произвольной структурой доступа.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Раздел 3. Блочные шифры и электронные подписи			
Тема 3.1. Симметричные блочные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.2. Шифрование с открытым ключом	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.3. Электронная подпись	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Раздел 4. Протоколы аутентификации и передачи ключей			
Тема 4.1. Протоколы аутентификации	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование
Тема 4.2. Протоколы с нулевым разглашением	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 4.3. Протоколы передачи ключей	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рацеев Сергей Михайлович. Математические методы защиты информации : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 543 с. - (Высшее образование). - ISBN 978-5-8114-8589-5 (в пер.). / .— ISBN 1_258181

2. Рябко Б.Я. Криптографические методы защиты информации : учебное пособие / Б.Я. Рябко, А.Н. Фионов ; Рябко Б.Я.; Фионов А.Н. - Москва : Горячая линия - Телеком, 2012. - 229 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991202862.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0286-2. / .— ISBN 0_242519

дополнительная

1. Рацеев Сергей Михайлович. Математические методы защиты информации и их основы. Сборник задач : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 136 с. - (Высшее образование). - Библиогр.: с. 135-136. - ISBN 978-5-507-45197-5 (в пер.). / .— ISBN 1_258183

2. Рябко Б.Я. Основы современной криптографии и стеганографии : монография / Б.Я. Рябко, А.Н. Фионов ; Рябко Б.Я.; Фионов А.Н. - Москва : Горячая линия - Телеком, 2010. - 232 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991201506.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0150-6. / .— ISBN 0_242509

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - 2022. - 11 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13333. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_475957.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Visual studio code

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная

электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и

инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доктор физико-математических наук, Доцент	Рацеев Сергей Михайлович
	Должность, ученая степень, звание	ФИО