Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ
Проректор по образовательной и
международной деятельности
_____ /А.А. Кирсанкин /
«____» _____ 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

(наименование дисциплины)

образовательной программы высшего образования –

программы специалитета

«**10.05.03 – Информационная безопасность автоматизированных систем**»

Специализация (Специализация №5):

«**Безопасность открытых информационных систем**»

Форма обучения: очная

Курган 2026

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»), утвержденным для очной формы обучения _26___ ___июня_____ 2026 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 03 июля 2026 года, протокол № 12.

Рабочую программу составил:
канд. пед. наук, доцент _____ /Т.А. Никифорова/

Согласовано:

Зав. кафедрой «БИАС»
канд. тех. наук, доцент _____ /Д.И. Дик/

Начальник Управления
образовательной деятельности _____ /И.В. Григоренко/

Специалист по учебно-методической
работе учебно-методического отдела _____ /Г.В. Казанкова/

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 5 зач. единиц трудоемкости (180 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**96**	**96**
Лекции	32	32
Лабораторные работы	32	32
Практические занятия	32	32
Самостоятельная работа, всего часов, в том числе:	**84**	**84**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	57	57
Вид промежуточной аттестации	**экзамен**	**экзамен**
	180	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательным дисциплинам Блока 1 - «Информационная безопасность».

Краткое содержание. Криптология: криптография и криптоанализ. Криптография и проблемы безопасности информации: конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства. Основные понятия криптографии: шифр, ключ, криптосистема, шифрование, дешифрование и др. Правило Керкхоффса. Криптосистема. Структура криптосистемы. Криптостойкость. Классификация методов криптографической защиты информации. Перестановочные шифры. Подстановочные шифры. Потоковые шифры. Блочные шифры. Симметричное и ассиметричное шифрование. Симметричные криптоалгоритмы. Ассиметричные криптоалгоритмы. Принципы построения, описания и анализа криптографических алгоритмов. Сеть Фейштеля. Криптоалгоритмы на основе сети Фейстеля. Криптоалгоритмы на основе подстановочно-перестановочных сетей (SP-сети). Криптоалгоритмы со структурой "квадрат". Принципы построения и криптоанализ симметричных и ассиметричных систем защиты информации. Стандадарты криптографиеческой защиты информации. Хэш-функции.Электронная цифровая подпись или цифровая подпись. Алгоритмы цифровой подписи. Криптографические протоколы. ПО для шифрования данных.

Изучение дисциплины «Методы и средства криптографической защиты информации» основывается на базе таких дисциплин как «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Языки программирования», «Технологии и методы программирования», «Основы теории защиты информации». Знания и навыки, полученные при изучении дисциплины «Методы и средства криптографической защиты информации», широко используются обучающимися при изучении общепрофессиональных и специальных дисциплин, связанных с вопросами проектирования, разработки, эксплуатации и внедрения автоматизированных систем защиты информации.

Результаты обучения по дисциплине необходимы для выполнения выпускной квалификационной работы в части проектирования автоматизированных систем или модулей защиты информации с использованием криптографических методов защиты информации.

Освоение следующих компетенций на уровне не ниже порогового: способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов криптографической защиты информации с помощью криптографических методов, криптографических протоколов; изложение принципов подтверждения авторства путем применения электронно-цифровой подписи; рассмотрение примеров реализации этих методов (алгоритмов) на практике.

Задачами освоения дисциплины «Методы и средства криптографической защиты информации» являются:

- дать основы системного подхода к организации криптографической защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов, криптографических алгоритмов и криптографических протоколов;
- изучение основных математических методов, используемых в криптографии;
- изучение основных алгоритмов криптографической защиты информации для разработки программных модулей реализации этих алгоритмов.

Компетенции, формируемые в результате освоения дисциплины:

- с способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Методы и средства криптографической защиты информации», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Методы и средства криптографической защиты информации», индикаторы достижения компетенций ОПК-10, перечень оценочных средств

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1$_{ОПК-10}$	Знать: новые образцы программных, технических средств и возможности информационных технологий, направленных на криптографическую защиту информации	З (ИД-1 $_{ОПК-10}$)	Знает: новые образцы программных, технических средств и возможности информационных технологий, направленных на криптографическую защиту информации	Вопросы теста
2.	ИД-2 $_{ОПК-10}$	Уметь: применять криптографические протоколы и криптографические алгоритмы для передачи и хранения данных в	У (ИД-2 $_{ОПК-10}$)	Умеет: применять криптографические протоколы и криптографические алгоритмы для передачи и хранения данных в	Комплект имитационных задач

		распределенных информационных системах		распределенных информационных системах	
3.	ИД-З $_{ОПК-10}$	Владеть: способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	В (ИД-З $_{ОПК-10}$)	Владеет: способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Вопросы для сдачи экзамена

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаборатор. работы	Практич. занятия
семестр 4					
Рубеж 1	1	Криптология: криптография и криптоанализ	2	4	2
	2	Классификация методов и алгоритмов криптографической защиты информации	6		2
	Рубежный контроль №1 (тестирование)		1	-	
Рубеж 2	3	Симметричное шифрование. Симметричные криптосистемы	6	8	6
	4	Асимметричное шифрование. Асимметричные криптосистемы и протоколы	8	16	6
	Рубежный контроль 2 (тестирование)		-	-	***2***
Рубеж 3	5	Принципы построения и методы анализа на криптостойкость криптографических алгоритмов	3	-	3
	Рубежный контроль 3 (решение задач)		-	-	1
Рубеж 4	6	Криптографические протоколы. ЭЦП, ЦП	6	4	8
	Рубежный контроль 4 (тестирование)				2
Всего за семестр:			**32**	**32**	**32**

4.2. Содержание лекционных занятий

Тема 1. Криптология: криптография и криптоанализ.

Криптология: криптография и криптоанализ. История развития криптографии. Криптография и проблемы безопасности информации: конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства.

Основные понятия криптографии: шифр, ключ, криптосистема, шифрование, дешифрование и др. Основной объект криптографии. Криптосистема. Структура криптосистемы. Требования к криптосистемам. Правило Керкхоффа. Криптостойкость.

Виды угроз. Атака на шифр. Стойкость ключа. Сложность вскрытия шифра.

Математическая модель шифра. Теория секретности Шеннона. Частотные характеристики открытых сообщений.

Тема 2. Классификация методов криптографической защиты информации

Основные этапы становления криптографии как науки. Исторические шифры. Классификация шифров. Шифры замены, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и машинных шифров: шифр Цезаря, шифр простой замены, шифр Плейфера, шифр Полибия (полибианский квадрат), шифр Виженера, шифр «Поворотная решетка» (поворотная решетка Кордано), шифр Хилла, шифр Вернама, Enigma, шифр Хейглина. Способы их вскрытия.

Классификация методов криптографической защиты информации. Перестановочные шифры. Подстановочные шифры. Потоковые шифры. Блочные шифры. Симметричное и ассиметричное шифрование. Симметричные криптоалгоритмы. Ассиметричные криптоалгоритмы.

Основные направления использования криптографических методов.

Принципы построения, описания и анализа криптографических алгоритмов. Сеть Фейштеля. Криптоалгоритмы на основе сети Фейстеля. Криптоалгоритмы на основе подстановочно-перестановочных сетей (SP-сети). Криптоалгоритмы со структурой "квадрат". Электронная цифровая подпись. Криптографические протоколы.

Рубежный контроль №1 (тестирование)

Тема 3. Симметричное шифрование. Симметричные криптосистемы.

3.1. Блочные шифры. Понятие о блочном шифре. Замены и перестановки. Методы замены: моноалфавитная, полиалфавитная, гомофоническая. Методы перестановки. SP-сеть. Лавинный эффект. Сеть Файстеля (Фейстеля). Критоалгоритмы симметричного шифрования DES, ГОСТ 28147-89. Шифр ГОСТ 28147-89. Режимы шифрования. Композиция блочных шифров. Шифры SQUARE, AES. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ. Многократное шифрование и атака «встреча посередине».

3.2. Псевдослучайные последовательности и поточные шифры. Характеристики генераторов псевдослучайных последовательностей (ПСП, ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся

шифры. Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. Шифр Trivium. Нелинейные регистры сдвига. Другие поточные шифры, например, RC4.

3.3. Теория имитостойкости Симмонса и криптографические хэш-функции. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону. Понятие кода аутентификации и его свойства имитостойкости и секретности. Назначение и конструкция кодов аутентификации и защитных контрольных сумм.

Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций. Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра.

Стандарты на хэш-функции: ГОСТ Р 34.11-94, SHA-1. Схема Меркла-Дамгарда и ГОСТ Р 34.11-2012. Концепция «губка» и SHA-3. Коды аутентификации и способы их построения. HMAC.

Тема 4. Асимметричное шифрование. Асимметричные криптосистемы и протоколы.

4.1. Асимметричные (с открытым ключом) шифры. Преимущества и недостатки асимметричных систем шифрования. Генерация ключевой информации для асимметричных криптосистем.

Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассера. Рюкзачные шифры. Криптосистемы с открытым ключом, основанные на линейных кодах. Вероятностные тесты на простоту. Доказуемо простые числа. Нахождение порождающего элемента и элемента заданного порядка.

4.2. Схемы цифровой подписи. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-Гамаля, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.

4.3. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой. Шифр Эль-Гамаля на эллиптической кривой. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ECDSA.

4.4. Введение в криптографические протоколы. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы вы-

работки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым разглашением на основе NP-сложных задач.

Тема 5. Принципы построения и методы анализа на криптостойкость криптографических алгоритмов.

Принципы построения и криптоанализ симметричных систем. Криптоанализ шифров перестановки. Криптоанализ открытых текстов.

Принципы построения и криптоанализ RSA. Атака методом Ферма. Атака повторным шифрованием. Атака на основе китайской теоремы об остатках. Бесключевое чтение.

Тема 6. Криптографические протоколы. ЭЦП, ЦП.

Введение в протоколы. Протоколы с посредником. Арбитражные протоколы. Самодостаточные протоколы. Попытки вскрытия протоколов.

Электронно-цифровая подпись на основе схем с открытыми ключами: RSA; схема Рабина; схема Шнорра; схема Эль-Гамаля; схема Фейге-Фиата-Шамира. Алгоритм цифровой подписи DSA. Российские стандарты ЭЦП. Стандарт цифровой подписи ГОСТ Р 34.10 – 2001. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ECDSA.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
4 семестр			
1	Криптология: криптография и криптоанализ	*Лабораторная работа №1.* Программное обеспечение для симметричного и асимметричного шифрования сообщений. Шифрующая файловая система (Encrypting File System - EFS).	2
		Лабораторная работа №2. Исследование функциональных возможностей криптосистемы PGP	2
3	Симметричное шифрование. Симметричные криптосистемы	*Лабораторная работа №3.* Виды симметричных систем. Методы замены: моноалфавитная, полиалфавитная, гомофоническая. Симметричные системы. Шифр Виженера. Шифр Плейфера. Битовые манипуляции.	4
		Лабораторная работа №4. Алгоритм ГОСТ 28147-89 и DES	4
4	Асимметричное шифрование. Асимметричные криптосистемы и протоколы	*Лабораторная работа №5.* Шифросистема RSA или криптосистема RSA	4
		Лабораторная работа №6. Вероятностное шифрование. Шифросистема Эль-Гамаля	4
		Лабораторная работа №7. Хеш-функции в криптографии. Программная реализация алгоритма хеш-функции	4

		Лабораторная работа №8. Программная реализация ЭЦП и стандартов ЭЦП.	4
6	Криптографические протоколы. ЭЦП	*Лабораторная работа №9.* Криптографические протоколы.	2
		Лабораторная работа 10. Электронно-цифровая подпись.	2
		Всего за семестр	**32**

4.4. Практические занятия

Номер темы	Наименование темы	Наименование практических занятий	Норматив времени, час.
		4 семестр	
1	Криптология: криптография и криптоанализ	*Практическая работа № 1.* Виды угроз. Атака на шифр. Стойкость ключа. Сложность вскрытия шифра.	1
		Практическая работа № 2. Математическая модель шифра. Теория секретности Шеннона. Частотные характеристики открытых сообщений.	1
2	Классификация методов криптографической защиты информации	*Практическая работа № 3.* Исторические шифры и их криптоанализ. Компьютерная реализация и вскрытие шифров замены и шифров перестановок.	2
3	Симметричное шифрование. Симметричные криптосистемы	*Практическая работа № 4.* Блочное симметричное шифрование	2
		Практическая работа № 5. Критоалгоритмы симметричного шифрования DES, ГОСТ 28147-89	4
4	Асимметричное шифрование. Асимметричные криптосистемы и протоколы	*Практическая работа № 6.* Алгоритм обмена ключами Диффи–Хеллмана.	2
		Практическая работа № 7. Алгоритм на основе задачи об укладке рюкзака (Knapsack Cryptosystem)	2
		Практическая работа № 8. Асимметричное шифрование, использующее эллиптические кривые	2
		Рубежный контроль 2 (тестирование)	***2***
5	Принципы построения и методы анализа на криптостойкость криптографических алгоритмов	*Практическая работа № 9.* Криптоанализ симметричных систем. Криптоанализ шифров замены и шифров перестановки..	1
		Практическая работа № 10. Победитель AES – шифр Rijndael	2
		Рубежный контроль3 (решение задач)	***1***
6	Криптографические протоколы. ЭЦП, ЦП	*Практическая работа № 11* Электронно-цифровая подпись. Цифровая подпись. Стандарты	4
		Практическая работа № 12. Криптографические протоколы.	4
		Рубежный контроль4 (тестирование)	***2***
		Всего за семестр	**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Преподавателем запланировано использование технологии учебной дискуссии при чтении лекций. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения в конце лекции в форме дискуссии.

Залогом качественного выполнения практических работ и лабораторных работ является самостоятельная подготовка к ним накануне путем повторения теоретических материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем перед началом работы.

Преподавателем запланировано применение на практических занятиях и лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях и лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к практическим занятиям и лабораторным работам, к рубежным контролям, подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение разделов	**25**
Подготовка к практическим занятиям и лабораторным работам (по 2 часа к каждому занятию)	24
Подготовка к рубежному контролю (по 2ч к каждому рубежу)	8
Подготовка к экзамену	27
Всего:	**84**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ.
2. Отчеты обучающихся по лабораторным работам.
3. Отчеты обучающихся по практическим занятиям.
4. Тестовые задания к рубежным контролям № 1, № 2, №3, №4.
5. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	*Распределение баллов, 4 семестр*						
		Вид учебной работы:	Посещение лекций	Выполнение практических работ	Выполнение и защита лабораторных работ	Рубежный контроль №1 и 2	Рубежный контроль №3 и 4	Экзамен
		Балльная оценка:	$0,5_б$х16= $8_б$	$2_б$ х 12 = $24_б$	$3_б$ х 10 =30	2+2	2+2	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета (экзамена)	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично						

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контролей не менее 51 балла. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения экзамена без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежных контролей. При этом, на усмотрение преподавателя, балльная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог балльной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 51 балла, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной практической или лабораторной работы (при невозможности дополнительного проведения работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 10 баллов; - прохождение рубежного контроля (баллы начисляются в зависимости от рубежного контроля) в дистанционной системе КГУ. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования или решения задач.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят

из 15 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 2 академических часа.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Экзамен проводится в форме ответа на вопросы билета. Экзаменационный билет состоит из 2 теоретических вопросов и 1 практического задания. Первые два вопроса оценивается в 10 баллов и практическое задание оценивается в 10 баллов. Вопросы к экзамену доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающемуся отводится 1 астрономический час.

Результаты текущего контроля успеваемости, экзамена заносятся преподавателем в экзаменационную ведомости, которые сдаются в орготдел институты в день экзамена, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежных контролей, экзамена

1-ый рубежный контроль

1. **Криптоанализ – это процесс, при котором**
   a. зная зашифрованное сообщение, пытаются узнать незашифрованное сообщение
   b. зная одну или несколько пар (незашифрованное сообщение, зашифрованное сообщение), пытаются узнать ключ
   c. изменяют передаваемое зашифрованное сообщение
2. **Что из перечисленного относится к механизмам безопасности ?**
   a. хэш-функции
   b. целостность сообщения
   c. алгоритмы симметричного шифрования
   d. невозможность отказа от полученного сообщения
3. **Целостность – это**
   a. невозможность несанкционированного просмотра информации
   b. невозможность несанкционированного изменения информации
   c. невозможность несанкционированного доступа к информации
4. **Побитовый XOR блоков нельзя считать криптографической хэш-функцией, потому что**
   a. противник может легко подобрать другое сообщение, имеющее тот же хэш-код

b. побитовый XOR плохо защищает от случайного сбоя
c. побитовый XOR требует сложных вычислений

5. **Для шифрования сообщения следует использовать**
   a. свой открытый ключ
   b. открытый ключ получателя
   c. свой закрытый ключ

2-ой рубежный контроль

1. **Самое быстрое шифрование/дешифрование**
   a. Rijndael
   b. MARS
   c. Serpent
   d. RC6
   e. Twofish
2. **Алгоритм ГОСТ 28147**
   a. имеет переменную длину ключа
   b. основан на сети Фейстеля
   c. разбивает блок на фиксированные 16-битные подблоки
3. **В алгоритмах симметричного шифрования используются только следующие операции:**
   a. операции перестановки и сдвига
   b. S-box и побитовое исключающее или (XOR)
   c. любые из перечисленных выше операций, а также многие другие
4. **Длина блока в алгоритме Rijndael может быть**
   a. 128 бит
   b. 192 бита
   c. 256 бит

3-ый рубежный контроль

1. Если в криптосистеме и для шифрования, и для дешифрования используется один и тот же ключ, то она называется

1) Криптосистемой с открытым ключом
2) Симметричной криптосистемой
3) Безопасной криптосистемой
4) Опасной криптосистемой

2. Характеристика шифра, определяющая его устойчивость к дешифрованию без знания ключа называется

1) Криптостойкостью
2) Тайной шифра
3) Вероятностью раскрытия шифра

3. Для современных криптографических систем защиты информации одним из общепринятых требований является

1) Зашифрованное сообщение ни кем не должно быть прочитано
2) Зашифрованное сообщение должно поддаваться чтению только при наличии ключа

3) Зашифрованное сообщение не должно поддаваться чтению даже при наличии ключа

4-ый рубежный контроль

1. Сообщение (3,1,2), закодированное с помощью ключа {7} по mod m = 33 алгоритмом RSA, имеет вид:

1) (19, 2, 21) 2) (3, 4, 8) 3) (3, 1, 16) 4) (9, 1, 29)

2. Сообщение «70», зашифрованное с помощью алгоритма «рюкзака» с ключом {2, 3, 6, 13, 27,52}, имеет вид:

1) 110101 2) 101011 3) 110010 4) 010100

3. Зашифровать сообщение методом Виженера (Ключ «Евгений_Онегин»)

МОЙ_ДЯДЯ_САМЫХ_ЧЕСТНЫХ_ПРАВИЛ,
КОГДА_НЕ_В_ШУТКУ_ЗАНЕМОГ,
ОН_УВАЖАТЬ_СЕБЯ_ЗАСТАВИЛ
И_ЛУЧШЕ_ВЫДУМАТЬ_НЕ_МОГ.

4 .Хэш-функция должна обладать следующими свойствами:

a. для любого данного значения хэш-кода h вычислительно невозможно найти M такое, что H (M) = h
b. хэш-функция H должна применяться к блоку данных фиксированной длины
c. хэш-функция H создает выход фиксированной длины

5. Выберите правильное утверждение

a. должно быть вычислительно невозможно подделать цифровую подпись как созданием нового сообщения для существующей цифровой подписи, так и созданием ложной цифровой подписи для некоторого сообщения
b. цифровая подпись должна быть достаточно компактной и не занимать много памяти
c. подпись обязательно должна быть рандомизированной

Примерная тематика вопросов, выносимых на экзамен в 4-ом семестре

1. Криптология: криптография и криптоанализ. История развития криптографии. Криптография и проблемы безопасности информации: конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства. Основные понятия криптографии: шифр, ключ, криптосистема, шифрование, дешифрование и др.
2. Криптосистема. Структура криптосистемы. Требования к криптосистемам. Правило Керкхоффа. Криптостойкость.
3. Виды угроз. Атака на шифр. Стойкость ключа. Сложность вскрытия шифра.
4. Математическая модель шифра. Теория секретности Шеннона. Частотные характеристики открытых сообщений.
5. Исторические шифры. Классификация шифров. Шифры замены, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и

машинных шифров: шифр Цезаря, шифр простой замены, шифр Плейфера, шифр Полибия (полибианский квадрат), шифр Виженера, шифр «Поворотная решетка» (поворотная решетка Кордано), шифр Хилла, шифр Вернама, Enigma, шифр Хейглина. Способы их вскрытия.

6. Классификация методов криптографической защиты информации. Перестановочные шифры. Подстановочные шифры. Потоковые шифры. Блочные шифры. Симметричное и ассиметричное шифрование. Симметричные криптоалгоритмы. Ассиметричные криптоалгоритмы.

7. Принципы построения, описания и анализа криптографических алгоритмов. Сеть Фейштеля. Криптоалгоритмы на основе сети Фейстеля. Криптоалгоритмы на основе подстановочно-перестановочных сетей (SP-сети). Криптоалгоритмы со структурой "квадрат". Электронная цифровая подпись. Криптографические протоколы.

8. Симметричное шифрование. Симметричные криптосистемы. Блочные шифры. Понятие о блочном шифре. Замены и перестановки. Методы замены: моноалфавитная, полиалфавитная, гомофоническая. Методы перестановки. SP-сеть. Лавинный эффект. Сеть Файстеля (Фейстеля).

9. Критоалгоритмы симметричного шифрования DES, ГОСТ 28147-89. Шифр ГОСТ 28147-89. Режимы шифрования.

10. Симметричное шифрование. Симметричные криптосистемы. Псевдослучайные последовательности и поточные шифры. Характеристики генераторов псевдослучайных последовательностей (ПСП, ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры. Регистры сдвига с обратной линейной связью (РСЛОС). ПСГ на основе РСЛОС. поточные шифры, например, RC4.

11. Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций. Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра.

12. Стандарты на хэш-функции: ГОСТ Р 34.11-94, SHA-1. Схема Меркла-Дамгарда и ГОСТ Р 34.11-2012. Концепция «губка» и SHA-3. Коды аутентификации и способы их построения. HMAC.

13. Асимметричное шифрование. Асимметричные (с открытым ключом) шифры. Преимущества и недостатки асимметричных систем шифрования. Генерация ключевой информации для асимметричных криптосистем. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.

14. Асимметричное шифрование. Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассера.

15. Рюкзачные шифры. Криптосистемы с открытым ключом, основанные на линейных кодах.

16. Схемы цифровой подписи. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП. Алгоритмы ЭЦП: RSA, Эль-

Гамаля, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.

17. Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Z_p к шифру (ЭЦП) на эллиптической кривой. Шифр Эль-Гамаля на эллиптической кривой.

18. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ECDSA.

19. Криптографические протоколы. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Парольные схемы и протоколы "рукопожатия". Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Вопросы организации сетей засекреченной связи. Доказательства с нулевым разглашением. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым разглашением на основе NP-сложных задач.

20. Принципы построения и криптоанализ симметричных систем. Криптоанализ шифров перестановки. Криптоанализ открытых текстов.

21. Принципы построения и криптоанализ RSA. Атака методом Ферма. Атака повторным шифрованием. Атака на основе китайской теоремы об остатках. Бесключевое чтение.

22. Электронно-цифровая подпись на основе схем с открытыми ключами: RSA; схема Рабина; схема Шнорра; схема Эль-Гамаля; схема Фейге-Фиата-Шамира. Алгоритм цифровой подписи DSA. Российские стандарты ЭЦП. Стандарт цифровой подписи ГОСТ Р 34.10 – 2001. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ECDSA.

23. Криптографические протоколы. Введение в протоколы. Протоколы с посредником. Арбитражные протоколы. Самодостаточные протоколы.

24. Попытки вскрытия протоколов.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. Математические аспекты. [Электронный ресурс]: Учебник. В 2

частях. — М. : Издательство Юрайт, 2016. – 210 с. URL: https://elibrary.ru/item.asp?id=25859687

2. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. [Электронный ресурс]: Учебное пособие - Москва: МИФИ, 2012. – 400 с. – Доступ из ЭБС «znanium.com».

3. Бабаш А.В. Криптографические методы защиты информации [Электронный ресурс]: учебник / А.В. Бабаш, Е.К. Баранова. — М. : КНОРУС, 2016. –190 с. URL:https://www.intuit.ru/studies/courses/16655/1300/lecture/25505?page=2.

4. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации [Электронный ресурс]: Учебное пособие для вузов. 2-е издание, стереотип. - М.: Горячая линия-Телеком, 2014. – 229 с. – Доступ из ЭБС «znanium.com».

5. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронно-цифровой подписи на базе асимметричного криптографического алгоритма [Электронный ресурс]: – Доступ из ЭБС «Консультант студента».

6. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи [Электронный ресурс]: – Доступ из ЭБС «Консультант студента».

7.2 Дополнительная литература:

1. Запечников, С. В. Криптографические методы защиты информации [Электронный ресурс]: учеб. пособие для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Издательство Юрайт, 2015. – 309 с. – Доступ из ЭБС «znanium.com».

2. Введение в криптографию. Под общей редакцией В. В. Ященко. [Электронный ресурс]: Издание 4-е, дополненное. МЦНМО, М., 2012. – 315 с. URL:https://edu-lib.com/matematika-2/dlya-studentov/vvedenie-v-kriptografiyu-pod-red-v-v-yashhenko-onlayn.

7.3 Методические материалы

1. Никифорова Т.А. Методические указания к практическим занятиям по дисциплине «Криптографические методы защиты информации» для студентов очной формы обучения направлений 10.05.03, 10.03.01. – Курган : КГУ, 2017. – 32 с.

2. Никифорова Т.А. Методические указания к выполнению контрольной работы по дисциплине «Криптографические методы защиты информации» для студентов очной формы обучения направлений 10.05.03, 10.03.01. – Курган : КГУ, 2017. – 29 с.

3. Никифорова Т.А. Лабораторный практикум «Криптоанализ классических шифров» для студентов специальностей 10.05.03, 10.03.01 и 09.03.04 по дисциплине «Криптографические методы защиты информации» для студентов очной формы обучения направлений 10.05.03, 10.03.01 и 09.03.04. – Курган : КГУ, 2016. – 57 с.

4. Никифорова Т.А. Задания к лабораторным работам по дисциплине «Криптографические методы защиты информации» для студентов очной формы обучения направлений 10.05.03, 10.03.01. – Курган : КГУ, 2017. – 18 с.

5. Никифорова Т.А. Методические указания к выполнению лабораторных работ по теме «Алгоритм RSA» для студентов очной формы обучения направлений 10.05.03, 10.03.01. – Курган : КГУ, 2016. – 96 с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт дистанционного обучения в НОУ (Национальный Открытый Университет) «ИНТУИТ» содержит бесплатные курсы, программы повышения квалификации и профессиональной переподготовки, интересные доклады и другую полезную информацию http://www.intuit.ru.
2. Федеральный портал «Российское образование» http://www.edu.ru/
3. Информационный сайт, содержащий справочные материалы по информатике, которые включают в себя курс лекций, схемы, презентации, рефераты и др. informatikaplus.narod.ru.
4. Сайт о высоких технологиях, новости индустрии из мира компьютерного «железа», тестовые испытания и обзоры оборудования IXBT.com.
5. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.

9 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн.

Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1.

Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения.

Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Криптографические методы защиты информации»

образовательной программы высшего образования –
программы специалитета
10.05.03 - Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем

Форма обучения: очная

Трудоемкость дисциплины: 5 з.е. (180 академических часа)
Семестр: 4 (очная форма обучения)
Форма промежуточной аттестации: экзамен
Содержание дисциплины. Основные разделы.

Криптология: криптография и криптоанализ. Криптография и проблемы безопасности информации: конфиденциальность, целостность, аутентификация, невозможность отказа сторон от авторства. Основные понятия криптографии: шифр, ключ, криптосистема, шифрование, дешифрование и др. Правило Керкхоффса. Криптосистема. Структура криптосистемы. Криптостойкость. Классификация методов криптографической защиты информации. Перестановочные шифры. Подстановочные шифры. Потоковые шифры. Блочные шифры. Симметричное и ассиметричное шифрование. Симметричные криптоалгоритмы. Ассиметричные криптоалгоритмы. Принципы построения, описания и анализа криптографических алгоритмов. Сеть Фейштеля. Криптоалгоритмы на основе сети Фейстеля. Криптоалгоритмы на основе подстановочно-перестановочных сетей (SP-сети). Криптоалгоритмы со структурой "квадрат". ПО для шифрования данных. Принципы построения и криптоанализ симметричных и ассиметричных систем защиты информации. Стандадарты криптографиеческой защиты информации. Хэш-функции. Электронная цифровая подпись или цифровая подпись. Алгоритмы цифровой подписи. Криптографические протоколы.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины
«Методы и средства криптографической защиты информации»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Никифорова Т.А./

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Никифорова Т.А./

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.