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
Первый проректор
_____ /Т.Р. Змызгова /
«__» августа 2022 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 2022

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 30 августа 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 августа 2022 года, протокол № 1.

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)	21	21
Курсовая работа	36	36
Вид промежуточной аттестации	**экзамен**	**экзамен**
	180	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Методы и средства криптографической защиты информации» относится к базовым 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 студентами 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 курсовой работы по дисциплине «Методы и средства криптографической защиты информации», а также 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).

В результате изучения дисциплины обучающийся должен:

знать:

- новые образцы программных, технических средств и возможности информационных технологий, направленных на криптографическую защиту информации (для ОПК-10);
- критерии оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (для ОПК-10);

уметь:

- проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (для ОПК-10);
- применять криптографические протоколы и криптографические алгоритмы для передачи и хранения данных в распределенных информационных системах (для ОПК-10);

владеть:

- способностью к освоению новых образцов программных, технических средств и информационных технологий (для ОПК-10);
- способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (для ОПК-10);
- способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (для ОПК-10).

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 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.

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. Стан-

дарт 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

Номер темы	Наименование темы	Наименование практических занятий	Норматив времени, час.
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 контроль 3 (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 контроль 4 (тестирование)		***2***
	Всего за семестр		**32**

4.5. Курсовая работа

Целью курсовой работы является реализация полученных знаний по основам криптографической защиты информации.

Курсовая работа выполняется в соответствии с индивидуальным заданием. Объем курсовой работы 20-25 страниц.

Структура курсовой работы:

1). Титульный лист.

2). Оглавление (содержание) курсовой работы/курсового проекта.

3). Введение.

4). Постановка задачи:

а) исходные данные;

б) цель курсовой работы;

в) задачи, подлежащие рассмотрению (решению) в курсовой работе.

5). Содержательная часть (может быть в виде двух глав, разделов, параграфов, привязанных к задачам курсовой работы).

6). Заключение и выводы:

а) перечень полученных результатов (согласно цели и задачам курсовой работы) и их новизна;

б) выводы, полученные по итогам курсовой работы.

ТЕМАТИКА КУРСОВЫХ РАБОТ ПО ДИСЦИПЛИНЕ

1. Программная реализация асимметричных криптографических алгоритмов.
2. Разработка программы аутентификации пользователей:
   - 2.1. Парольная аутентификация с дополнительными средствами администрирования (задание максимального и минимального сроков действия пароля, ведение списка уже использованных паролей задаваемой максимальной длины).
   - 2.2. Аутентификация пользователей на основе модели «рукопожатия».
   - 2.3. Аутентификация пользователей по их «росписи» мышью.
   - 2.4. Аутентификация пользователей по их клавиатурному почерку.
   - 2.5. Аутентификация пользователей на основе их способности к запоминанию отображаемой на короткое время на экране информации.
3. Хэш-функции. Алгоритм MD5. Стандарты SHA, ГОСТ Р 34.11-94.
4. Блочные шифры. SP-сети. Принцип итерирования. Конструкция Фейстеля. Примеры (ГОСТ 28147-89, AES).
5. Математические методы квантовой криптографии.
6. Режимы работы DES. Сцепление блоков. Шифрованная обратная связь. Двойной и тройной DES. Другие симметрично-блочные шифры.
7. Поточное шифрование. Регистры сдвига. Примеры шифров (A5, RC4).
8. Модулярные шифры. Шифры Вижинера.
9. «Плотные рюкзачные криптосистемы» с элементами из конечных полей.
10. Электронные платежи.
11. Цифровая подпись документа (аутентификация).
12. Оценка качества генераторов псевдослучайных последовательностей, используемых в поточных шифрах.
13. LLL-алгоритм построения приведенного базиса решетки: программная реализация, применение в криптографии.
14. Исследование зависимостей производительности вычислений типовых операций над точками эллиптической кривой от систем координат, в которых рассматривается эллиптическая кривая.
15. Алгоритмы факторизации (разложения на простые множители) целых составных чисел: Алгоритм Ленстры, ρ-метод Полларда, Парадокс дней рождения и др.
16. Методы решения задач дискретного логарифмирования: Метод полного перебора, алгоритм Сильвера-Полига-Хеллмана и др.
17. Методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов.
18. Прикладная теория автоматов – автоматные модели криптосистем и управляющих систем.
19. Логическое проектирование дискретных автоматов – математические модели и методы анализа, синтеза, оптимизации и оценки сложности дискретных автоматов, аппаратная реализация криптоалгоритмов.
20. Управление ключами. Генерация ключей. Распределение ключей. Инфраструктура открытого ключа. Централизованное (центры сертификации) и распределенное управление.

21. Системы с открытым распределением ключей для абонентских сетей.
22. Разделение секрета на основе уравнений Лагранжа. Разделение секрета на основе китайской теоремы об остатках. Разделение секрета на основе свойств равновесных кодов.
23. Разработка программных средств компьютерной стеганографии:
    23.1. Скрытие и извлечение информации в графических файлах.
    23.2. Скрытие и извлечение информации в звуковых файлах.
    23.3. Скрытие и извлечение информации в видеофайлах.
    23.4. Скрытие и извлечение информации в текстовых файлах.
24. Разработка защищенной почтовой клиентской программы:
    24.1. С автоматическим шифрованием (расшифрованием) сообщений и (или) присоединенных к ним файлов.
    24.2. С автоматическим получением ЭЦП под сообщением и (или) присоединенных к нему файлов (при отправке сообщения) и проверкой ЭЦП (при получении сообщения).
    24.3. С автоматической проверкой на вредоносные вложения с помощью одной из программ-сканеров.
25. Комбинированное шифрование на основе алгоритмов Rijndael и MARS.
26. Разработка алгоритма внедрения цифрового водяного знака в изображение.
27. Защита информации в электронных платежных системах на основе алгоритма определения принадлежности числа интервалу с нулевым разглашением.
28. Программная реализация алгоритмов хэширования SHA-1, SHA-256, SHA-384 и SHA-512.
29. Генерация и исследование криптографически стойких эллиптических кривых
30. Статистический анализ криптоалгоритмов.
31. Разработка программного комплекса «Лабораторный модуль «Экспериментальное исследование стойкости криптосистемы RSA».
32. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных.

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, или выполнения курсовой 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, написание курсовой работы, 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	-
Подготовка к практическим занятиям и лабораторным работам	13
Подготовка к рубежному контролю (по 2ч к каждому рубежу)	8
Курсовая работа	36
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 студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Курсовая работа.
5. Тестовые задания к рубежным контролям № 1, № 2, №3, №4.
6. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="8">Содержание</td></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="8">Распределение баллов, 4 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение практических работ</td><td>Выполнение и защита лабораторных работ</td><td>Рубежный контроль №1 и 2</td><td>Рубежный контроль №3 и 4</td><td>Экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$0,5_б$x16= $8_б$</td><td>$2_б$ x 12 = $24_б$</td><td>$3_б$ x 10 =30</td><td>2+2</td><td>2+2</td><td>30</td></tr>
<tr><td colspan="8">Курсовая работа (4 семестр)</td></tr>
<tr><td colspan="2">Качество пояснительной записки</td><td colspan="2">Качество программной части</td><td>Систематичность выполнения задания</td><td>антиплагиат</td><td>Качество защиты</td><td>Всего</td></tr>
<tr><td colspan="2">до 20</td><td colspan="2">до 30</td><td>до 10</td><td>До 10</td><td>до 30</td><td>100</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета (экзамена)</td><td colspan="8">60 и менее баллов – неудовлетворительно; не зачтено;
61…73 – удовлетворительно; зачтено;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="8">Для допуска к промежуточной аттестации (экзамену) студент должен набрать не менее 50 баллов, выполнить все практические, лабораторные, курсовую работы.
Для получения экзаменационной оценки «автоматически» и получить оценку «удовлетворительно» студенту необходимо набрать 68 баллов.
По согласованию с преподавателем студенту, набравшему минимум 68 балл, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях и лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена оценка «хорошо» или «отлично» автоматически.</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае, если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов (не выполнены все задания), необходимо выполнить дополнительные задания, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических и лабораторных работ. 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 системе KeSS 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 со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят из 15 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту 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 студента 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 студентов на последней лекции в семестре. На подготовку ответа студенту 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 студента.

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 моне-

ты. 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 криптографических 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

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Library Office.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

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

«Методы и средства криптографической 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.