Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.01.02 «МЕТОДЫ ОЦЕНКИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Сухотерин А.И. Рабочая программа дисциплины (модуля): Методы оценки криптографических систем защиты информации. – Королев МО: «Технологический Университет», 2023

Рецензент: Шихнабиева Т.Ш.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 год

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н. доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является:

Сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.

Освоение студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Профессиональные компетенции:

- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными **задачами** дисциплины являются:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.
- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной

ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

Необходимые знания:

- УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01. «Информационная безопасность».

Дисциплина базируется на ранее изученных дисциплинах: «Защищенные информационные системы», «Основы теории информационной безопасности», «Анализ статистической информации с помощью пакета прикладных программ» и компетенциях: УК-1; ОПК-1; ПК-1, 2, 3

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при для написания магистерской диссертации.

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 6 зачетные единицы, 216 часа.

Таблица1

Виды занятий	Всего часов	Семестр 3	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**216**	**216**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**46**	**46**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	24	24			
Лабораторные работы (ЛР)	-	-			
Другие виды контактной работы*	**6**	**6**			
Самостоятельная работа	**168**	**168**			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.					
Вид итогового контроля	Экзамен	Экзамен			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4.Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Третий семестр				
Раздел 1. Теоретические основы криптографии				
Тема 1. Общие принципы информационной безопасности.	4	6	3	УК-1 ПК-3
Тема 2. Теоретические основы криптографии.	4	6	3	УК-1 ПК-3
Раздел 2. Прикладные криптографические методы систем защиты информации и их реализация				

Тема 3. Криптографические протоколы.	4	6	3	УК-1 ПК-3
Тема 4. Общие принципы PKI.	4	6	3	УК-1 ПК-3
Итого:	16	24	12	

4.2. Содержание тем дисциплины

Раздел 1. Теоретические основы криптографии

Тема 1. Общие принципы информационной безопасности

Политика безопасности, уязвимости, угрозы, механизмы и услуги безопасности, превентивные и проактивные методы обеспечения безопасности. Принципы построения систем информационной безопасности: минимизация привилегий, минимальное число доверенных компонент, простота, скептицизм и параноидальный подход к оценке криптостойкости.

Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.

Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Тема 2. Теоретические основы криптографии

Формальное определение классической криптосистемы. Условная вероятность и теорема Байеса. Совершенная секретность и теорема Шеннона. Одноразовый блокнот (шифр Вернама). Конечные поля. Мультипликативная группа конечного поля. Дискретная логарифмическая проблема. Теоремы Эйлера и Ферма. Эллиптические кривые. Группа точек эллиптической кривой.

Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB,

PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамаля. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

Свойства хэш-функци. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHS, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Раздел 2. Прикладные криптографические методы систем защиты информации и их реализация

Тема 3. Криптографические протоколы

Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.

Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

Принципы квантовой криптографии. Квантовый протокол распределения ключей.

Обзор биометрических методов. Метод биометрической «вуали».

Тема 4. Общие принципы PKI

Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. Определения ключей Baffine.

Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSYD.

Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).

Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных

сертификатов (СОС), приостановление действия сертификата, Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура PKI. Понятие сертификационного пути. Преимущества PKI.

Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Проекты Clipper и Capstone. Стандарт EES. Криптоалгоритм Skipjack.

Проблематика. Промежуточные СОС (Delta CRL). Сегментированные СОС. Система отзыва сертификатов (CRS). Проверка статуса сертификата при помощи дерева Меркля. Протокол проверки статуса сертификата OCSP.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины (модуля)» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Методы оценки криптографических систем защиты информации» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **http://www.academy.it.ru/ –** академия АЙТИ.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды Университета
2. Информационно-справочные системы (Консультант+; Гарант)

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows XP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задание

ЗАДАНИЕ №1

(тема: Блочные шифры)

Цель работы

Используя любой язык программирования написать программу,

реализующую один из алгоритмов шифрования в соответствии с вариантом

задания. Исходный код программы, а также скриншот результата выполнения

прикрепить к данному занятию.

Задание

Произвести зашифровывание и расшифровывание произвольной фразы

произвольной длины с использованием произвольного ключа одним из

следующих симметричных алгоритмов шифрования (в соответствии с

номером варианта).

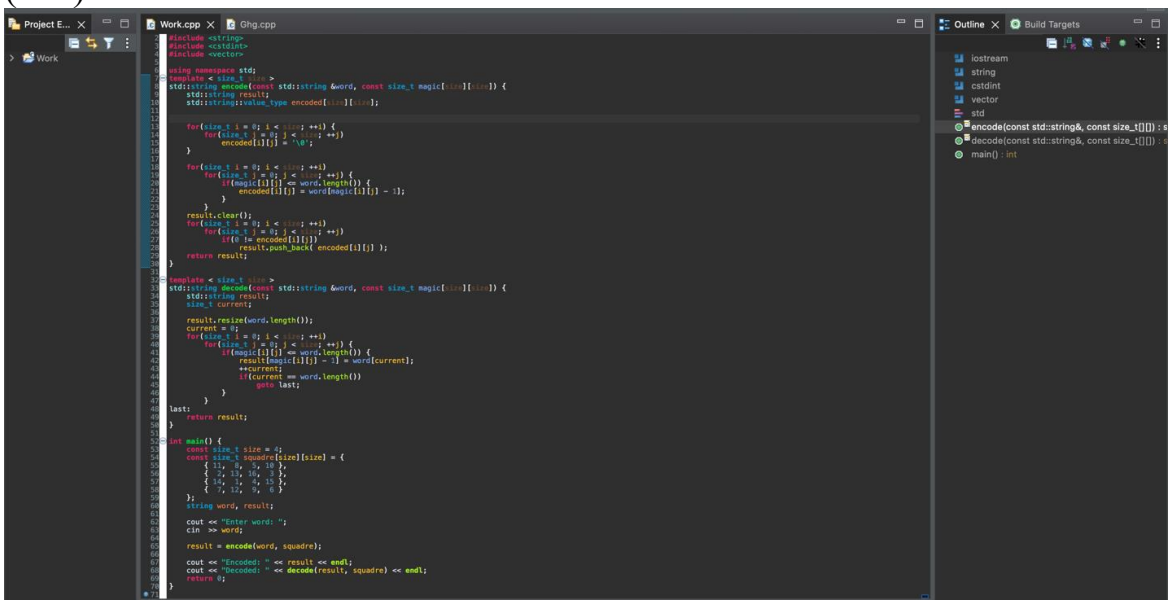
Произвести зашифровывание и расшифровывание произвольной фразы произвольной длины с использованием произвольного ключа одним из следующих симметричных алгоритмов шифрования (в соответствии с номером варианта):

1. шифр Цезаря
2. магический квадрат (4x4)
3. лозунговый шифр
4. простая одинарная перестановка

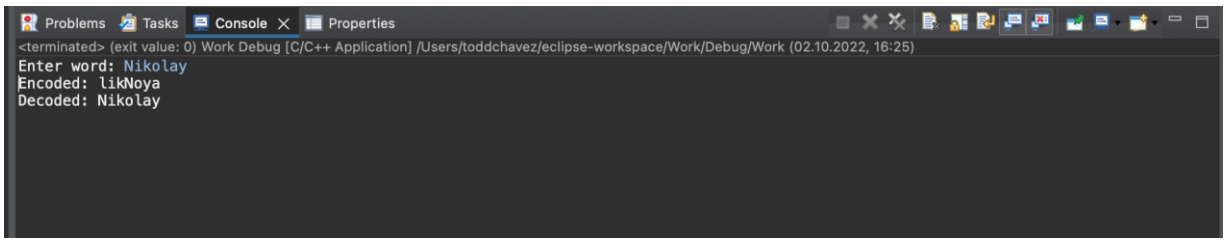
5. двойная перестановка
6. шифр Playfair
7. блочная одинарная перестановка
8. табличная маршрутная перестановка
9. вертикальная перестановка
10. полибианский квадрат
11. шифр Виженера
12. шифр Цезаря
13. магический квадрат (4x4)
14. лозунговый шифр
15. простая одинарная перестановка
16. двойная перестановка
17. шифр Playfair
18. блочная одинарная перестановка
19. табличная маршрутная перестановка
20. вертикальная перестановка
21. полибианский квадрат
22. шифр Виженера
23. шифр Цезаря
24. магический квадрат (4x4)
25. лозунговый шифр
26. простая одинарная перестановка
27. двойная перестановка

Практическая часть.

1. Архитектурное представления кода в соответствии с заданием. Программа шифрования на основе алгоритма магического квадрата (4x4) написана на ЯП C++.



2. Проверяем код на его корректность и на количество (если есть) логических ошибок.



3. Программа работает корректно и исправно.

Вывод:

Был написан алгоритм по кодированию и декодированию случайной последовательности букв (некого слова) на основе магического квадрата (4x4).

ЗАДАНИЕ №2
(тема: симметричное и асимметричное шифрование)

Произвести зашифровывание и расшифровывание произвольной фразы произвольной длины следующими алгоритмами шифрования:

1. DES
2. ГОСТ 28147-89
3. RSA
4. Эль-Гамаль
5. Эль-Гамаль
6. DES
7. RSA
8. ГОСТ 28147-89
9. RSA
10. DES
11. ГОСТ 28147-89
12. Эль-Гамаль
13. ГОСТ 28147-89
14. Эль-Гамаль
15. RSA
16. DES
17. RSA
18. DES
19. ГОСТ 28147-89
20. ГОСТ 28147-89
21. Эль-Гамаль
22. RSA

Цель работы

Используя любой язык программирования написать программу,

реализующую один из алгоритмов шифрования в соответствии с вариантом

задания. Исходный код программы, а также скриншот результата выполнения

прикрепить к данному занятию

```
#include <stdio.h>
#include <stdint.h>

// 10101100 << 2 = 10110000 | 00000010 = 10110010
#define LSHIFT_nBIT(x, L, N) (((x << L) | (x >> (-L & (N - 1)))) & (((uint64_t)1 << N) - 1))
// #define RSHIFT_nBIT(x, R, N) (((x >> R) | (x << (-R & (N - 1)))) & (((uint64_t)1 << N) - 1))

#define BUFF_SIZE 1024

size_t GOST_28147(uint8_t * to, uint8_t mode, uint8_t * key256b, uint8_t * from, size_t length);
void feistel_cipher(uint8_t mode, uint32_t * block32b_1, uint32_t * block32b_2, uint32_t * keys32b);
void round_of_feistel_cipher(uint32_t * block32b_1, uint32_t * block32b_2, uint32_t * keys32b, uint8_t round);

uint32_t substitution_table(uint32_t block32b, uint8_t sbox_row);
void substitution_table_by_4bits(uint8_t * blocks4b, uint8_t sbox_row);

void split_256bits_to_32bits(uint8_t * key256b, uint32_t * keys32b);
void split_64bits_to_32bits(uint64_t block64b, uint32_t * block32b_1, uint32_t * block32b_2);
void split_64bits_to_8bits(uint64_t block64b, uint8_t * blocks8b);
void split_32bits_to_8bits(uint32_t block32b, uint8_t * blocks4b);

uint64_t join_32bits_to_64bits(uint32_t block32b_1, uint32_t block32b_2);
uint64_t join_8bits_to_64bits(uint8_t * blocks8b);
uint32_t join_4bits_to_32bits(uint8_t * blocks4b);

static inline void print_array(uint8_t * array, size_t length);
static inline void print_bits(uint64_t x, register uint64_t Nbit);

// 1 | 4 -> 0xC
static const uint8_t Sbox[8][16] = {
```

```
            {0xF, 0xC, 0x2, 0xA, 0x6, 0x4, 0x5, 0x0, 0x7, 0x9, 0xE, 0xD, 0x1,
0xB, 0x8, 0x3},
            {0xB, 0x6, 0x3, 0x4, 0xC, 0xF, 0xE, 0x2, 0x7, 0xD, 0x8, 0x0, 0x5,
0xA, 0x9, 0x1},
            {0x1, 0xC, 0xB, 0x0, 0xF, 0xE, 0x6, 0x5, 0xA, 0xD, 0x4, 0x8, 0x9,
0x3, 0x7, 0x2},
            {0x1, 0x5, 0xE, 0xC, 0xA, 0x7, 0x0, 0xD, 0x6, 0x2, 0xB, 0x4, 0x9,
0x3, 0xF, 0x8},
            {0x0, 0xC, 0x8, 0x9, 0xD, 0x2, 0xA, 0xB, 0x7, 0x3, 0x6, 0x5, 0x4,
0xE, 0xF, 0x1},
            {0x8, 0x0, 0xF, 0x3, 0x2, 0x5, 0xE, 0xB, 0x1, 0xA, 0x4, 0x7, 0xC,
0x9, 0xD, 0x6},
            {0x3, 0x0, 0x6, 0xF, 0x1, 0xE, 0x9, 0x2, 0xD, 0x8, 0xC, 0x4, 0xB,
0xA, 0x5, 0x7},
            {0x1, 0xA, 0x6, 0x8, 0xF, 0xB, 0x0, 0x4, 0xC, 0x3, 0x5, 0x9, 0x7,
0xD, 0x2, 0xE},
        };

        int main(void) {
            uint8_t encrypted[BUFF_SIZE], decrypted[BUFF_SIZE];
            uint8_t key256b[32] = "this_is_a_pasw_for_GOST_28147_89";

            uint8_t buffer[BUFF_SIZE], ch;
            size_t position;
            while ((ch = getchar()) != '\n' && position < BUFF_SIZE - 1)
                buffer[position++] = ch;
            buffer[position] = '\0';

            printf("Open message:\n");
            print_array(buffer, position);
            printf("%s\n", buffer);
            putchar('\n');

            position = GOST_28147(encrypted, 'E', key256b, buffer, position);
            printf("Encrypted message:\n");
            print_array(encrypted, position);
            printf("%s\n", encrypted);
            putchar('\n');

            printf("Decrypted message:\n");
            position = GOST_28147(decrypted, 'D', key256b, encrypted,
position);
            print_array(decrypted, position);
            printf("%s\n", decrypted);
```

```
        putchar('\n');

        return 0;
    }

    size_t GOST_28147(uint8_t * to, uint8_t mode, uint8_t * key256b, uint8_t * from, size_t length) {
        length = length % 8 == 0 ? length : length + (8 - (length % 8));
        uint32_t N1, N2, keys32b[8];
        split_256bits_to_32bits(key256b, keys32b);

        for (size_t i = 0; i < length; i += 8) {
            split_64bits_to_32bits(
                join_8bits_to_64bits(from + i),
                &N1, &N2
            );
            feistel_cipher(mode, &N1, &N2, keys32b);
            split_64bits_to_8bits(
                join_32bits_to_64bits(N1, N2),
                (to + i)
            );
        }

        return length;
    }

    // keys32b = [K0, K1, K2, K3, K4, K5, K6, K7]
    void feistel_cipher(uint8_t mode, uint32_t * block32b_1, uint32_t * block32b_2, uint32_t * keys32b) {
        switch (mode) {
            case 'E': case 'e': {
                // K0, K1, K2, K3, K4, K5, K6, K7, K0, K1, K2, K3, K4, K5, K6, K7, K0, K1, K2, K3, K4, K5, K6, K7
                for (uint8_t round = 0; round < 24; ++round)
                    round_of_feistel_cipher(block32b_1, block32b_2, keys32b, round);

                // K7, K6, K5, K4, K3, K2, K1, K0
                for (uint8_t round = 31; round >= 24; --round)
                    round_of_feistel_cipher(block32b_1, block32b_2, keys32b, round);
                break;
            }
            case 'D': case 'd': {
```

```
                // K0, K1, K2, K3, K4, K5, K6, K7
                for (uint8_t round = 0; round < 8; ++round)
                    round_of_feistel_cipher(block32b_1, block32b_2, keys32b,
round);

                // K7, K6, K5, K4, K3, K2, K1, K0, K7, K6, K5, K4, K3, K2,
K1, K0, K7, K6, K5, K4, K3, K2, K1, K0
                for (uint8_t round = 31; round >= 8; --round)
                    round_of_feistel_cipher(block32b_1, block32b_2, keys32b,
round);
                break;
            }
        }
    }

    void round_of_feistel_cipher(uint32_t * block32b_1, uint32_t *
block32b_2, uint32_t * keys32b, uint8_t round) {
        uint32_t result_of_iter, temp;

        // RES = (N1 + Ki) mod 2^32
        result_of_iter = (*block32b_1 + keys32b[round % 8]) %
UINT32_MAX;

        // RES = RES -> Sbox
        result_of_iter = substitution_table(result_of_iter, round % 8);

        // RES = RES <<< 11
        result_of_iter = (uint32_t)LSHIFT_nBIT(result_of_iter, 11, 32);

        // N1, N2 = (RES xor N2), N1
        temp = *block32b_1;
        *block32b_1 = result_of_iter ^ *block32b_2;
        *block32b_2 = temp;
    }

    uint32_t substitution_table(uint32_t block32b, uint8_t sbox_row) {
        uint8_t blocks4bits[4];
        split_32bits_to_8bits(block32b, blocks4bits);
        substitution_table_by_4bits(blocks4bits, sbox_row);
        return join_4bits_to_32bits(blocks4bits);
    }

    void substitution_table_by_4bits(uint8_t * blocks4b, uint8_t sbox_row)
{
```

```
            uint8_t block4b_1, block4b_2;
            for (uint8_t i = 0; i < 4; ++i) {
                // 10101100 & 0x0F = 00001100
                // [example get from table] 1100 -> 1001
                block4b_1 = Sbox[sbox_row][blocks4b[i] & 0x0F];

                // 10101100 >> 4 = 00001010
                // [example get from table] 1010 -> 0111
                block4b_2 = Sbox[sbox_row][blocks4b[i] >> 4];

                // 00001001
                blocks4b[i] = block4b_2;

                // (00001001 << 4) | 0111 =
                // 1001000 | 0111 = 10010111
                blocks4b[i] = (blocks4b[i] << 4) | block4b_1;
            }
        }

        void split_256bits_to_32bits(uint8_t * key256b, uint32_t * keys32b) {
            uint8_t *p8 = key256b;
            // p32[0] = 00000000000000000000000000000000
            for (uint32_t *p32 = keys32b; p32 < keys32b + 8; ++p32) {
                // 00000000000000000000000000000000 << 8 | 10010010 =
00000000000000000000000010010010
                // 00000000000000000000000010010010 << 8 | 00011110 =
00000000000000001001001000011110
                // 00000000000000001001001000011110 << 8 | 11100011 =
00000000100100100001111011100011
                // 00000000100100100001111011100011 << 8 | 01010101 =
10010010000111101110001101010101
                for (uint8_t i = 0; i < 4; ++i) {
                    *p32 = (*p32 << 8) | *(p8 + i);
                }
                p8 += 4;
            }
        }

        void split_64bits_to_32bits(uint64_t block64b, uint32_t * block32b_1,
uint32_t * block32b_2) {
            //                                    N1                                    =
(uint32_t)0000101010101010101010101010101010101010101010101010101010101010
010101111 =
            // = 10101010101010101010101010101111
```

```
            *block32b_2 = (uint32_t)(block64b);

            //                                          N2                                          =
(uint32_t)00001010101010101010101010101010101010101010101010101010101010101
010101111 >> 32 =
            //                                                                                      =
(uint32_t)00000000000000000000000000001010101010101010101010101010101010101
01111 =
            // = 10101010101010101010101010101111
            *block32b_1 = (uint32_t)(block64b >> 32);
        }

        void split_64bits_to_8bits(uint64_t block64b, uint8_t * blocks8b) {
            for (size_t i = 0; i < 8; ++i) {
                // blocks8b[0] =
                //                                                                                  =
(uint8_t)00001010101010101010101010101010101010101010101010101010101010101010
10101111 >> ((7 - 0) * 8)
                //                                                                                  =
(uint8_t)00001010101010101010101010101010101010101010101010101010101010101010
10101111 >> 56 =
                //                                                                                  =
(uint8_t)00000000000000000000000000000000000000000000000000000000000000000000
00001010 =
                // = 00001010
                blocks8b[i] = (uint8_t)(block64b >> ((7 - i) * 8));
            }
        }

        void split_32bits_to_8bits(uint32_t block32b, uint8_t * blocks8b) {
            for (uint8_t i = 0; i < 4; ++i) {
                //  blocks8b[0]  =  (uint8_t)10111101000101010100101110100010
>> (28 - (0 * 8)) =
                // = (uint8_t)10101010101010101010101010101010 >> 28 =
                // = (uint8_t)00000000000000000000000010111101
                // = 10111101
                blocks8b[i] = (uint8_t)(block32b >> (24 - (i * 8)));
            }
        }

        /*
        // WRONG FUNCTION!
        void split_32bits_to_4bits(uint32_t block32b, uint8_t * blocks4b) {
            for (uint8_t i = 0; i < 4; ++i) {
```

```
            // blocks4b[0] = (uint8_t)10101010101010101010101010101010
>> (28 - (0 * 8)) =
            // = (uint8_t)10101010101010101010101010101010 >> 28 =
            // = (uint8_t)00000000000000000000000010101010
            // = 10101010
            blocks4b[i] = (uint8_t)(block32b >> (28 - (i * 8)));
            // blocks4b[0] = (10101010 << 4) |
(uint8_t)(10101010101010101010101010101010 & 0x0F) =
            // = (10101010 << 4) |
(uint8_t)(10101010101010101010101010101010 & 00001111) =
            // = 10100000 | (uint8_t)00000000000000000000000000001010
            // = 10100000 | 00001010 = 10101010
            blocks4b[i] = (blocks4b[i] << 4) | (uint8_t)(block32b & 0x0F);
        }
    }
    */

    uint64_t join_32bits_to_64bits(uint32_t block32b_1, uint32_t
block32b_2) {
        uint64_t block64b;
        // block64b = 10101010101010101010101010101010 =
        //
0000000000000000000000000000000010101010101010101010101010101010
0
        block64b = block32b_2;
        // block64b =
        //                                                                =
(0000000000000000000000000000000010101010101010101010101010101010
0 << 32) | 11111111111111111111111111111111 =
        //                                                                =
1010101010101010101010101010101000000000000000000000000000000000
0 | 11111111111111111111111111111111 =
        //                                                                =
10101010101010101010101010101011111111111111111111111111111111
        block64b = (block64b << 32) | block32b_1;
        return block64b;
    }

    uint64_t join_8bits_to_64bits(uint8_t * blocks8b) {
        uint64_t block64b;
        //                                  block64b                      =
0000000000000000000000000000000000000000000000000000000000000000
0
        for (uint8_t *p = blocks8b; p < blocks8b + 8; ++p) {
```

```
            // i = 0
            //
(00000000000000000000000000000000000000000000000000000000000000000 << 8) | 11001100 =
            //
0000000000000000000000000000000000000000000000000000000011001100
            // i = 1
            //
(0000000000000000000000000000000000000000000000000000000011001100 << 8) | 11110011 =
            //
0000000000000000000000000000000000000000000000001100110000000000 | 11110011 =
            //
0000000000000000000000000000000000000000000000001100110011110011
            // ... i < 8 ...
            block64b = (block64b << 8) | *p;
        }
        return block64b;
    }

    uint32_t join_4bits_to_32bits(uint8_t * blocks4b) {
        uint32_t block32b;
        // block64b = 00000000000000000000000000000000
        for (uint8_t i = 0; i < 4; ++i) {
            // i = 0
            // (00000000000000000000000000000000 << 8) | 11001100 =
            // 00000000000000000000000011001100
            // i = 1
            // (00000000000000000000000011001100 << 8) | 11110011 =
            // 00000000000000001100110000000000 | 11110011 =
            // 00000000000000001100110011110011
            // ... i < 4 ...
            block32b = (block32b << 8) | blocks4b[i];
        }
        return block32b;
    }

    static inline void print_array(uint8_t * array, size_t length) {
        printf("[ ");
        for (size_t i = 0; i < length; ++i)
            printf("%d ", array[i]);
```

```
    printf("]\n");
}

static inline void print_bits(uint64_t x, register uint64_t Nbit) {
    for (Nbit = (uint64_t)1 << (Nbit - 1); Nbit > 0x00; Nbit >>= 1)
        printf("%d", (x & Nbit) ? 1 : 0);
    putchar('\n');
}
```

Пример компилирования:
Nikolay
Open message:
[78 105 107 111 108 97 121]
Nikolay

Encrypted message:
[116 174 142 191 168 120 56 80]
t����x8P��`□

Decrypted message:
[78 105 107 111 108 97 121 0]
Nikolay

Вывод:

Был написан алгоритм по кодированию и декодированию случайной

последовательности букв (некого слова) на ГОСТ 28147-89. Вариант 13

ЗАДАНИЕ №3
(тема: Исследование создания сеансовых ключей на основе алгоритма Диффи-Хеллмана)

Цель работы

Изучить принципы генерации сеансовых ключей шифрования в ИС

Задание

1. Записать номер варианта N соответствующий младшей цифре студенческого билета

3. Определить простое число P по таблице простых числе следующим образом: номер числа P в таблице равен N+30

4. Заполнить таблицу 2 в соответствии с номером варианта

5. Выбрать произвольные не совпадающие значения чисел D, X1, X2 и

Таблица1. Таблица простых чисел

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Исследуемая величина		
Простое число P		
Мантисса 1<D<(P−1)		
Пользователи	Первый	Второй
Случайное 1<X_i<(P−1)		
$Y_1 = D^{X_1} \pmod P$ и $Y_2 = D^{X_2} \pmod P$		
Сеансовый ключ $K_{12} = Y_2^{X_1} \pmod P = Y_1^{X_2} \pmod P$		

Содержание работы

1. Записать в таблицу своё число P согласно номеру варианта
2. Записать значения D, X1, X2 и занести в таблицу
3. Вычислить в форме значения Y1 и Y2, занести их в таблицу
4. Вычислить в форме значения ключа K12 и занести в таблицу
5. Записать выводы

Практическая часть

Исследование создания сеансовых ключей на основе алгоритма Диффи-Хеллмана

Студент: Линев Н.В. Вариант: 1.

P = 127; N+30 = 1+30 = 31;
Мантисса: D = 120;

Пользователь 1. Пользователь 2.
X1 = 5;
X2 = 7;

Y1 = 84;
Y2 = 52;

K1 = 68;
K2 = 68.

Вывод:

Была произведена проверка сеансовых ключей на основе алгоритма Диффи-Хеллмана.

ЗАДАНИЕ №4
(тема: Создание электронной подписи)

Цель работы

Изучить принципы создания электронной подписи

Задание

1. Определить простые числа по таблице простых чисел по следующему алгоритму:

- номер первого простого числа, требующегося для создания ЭП в соответствии с алгоритмом, соответствует номеру варианта по списку;
- номер второго простого числа соответствует номеру варианта + 5;
- номера следующих простых чисел (при необходимости) определяются путем прибавления + 5 к номеру предыдущего простого числа.

2. Используя алгоритмы, соответствующие номеру варианта, сформировать электронную подпись

3. Сравнить полученные результаты

Таблица1. Таблица простых чисел

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Варианты заданий:
1. RSA, DSA
2. RSA, ГОСТ Р 34.10-94
3. RSA, Эль-Гамаль
4. Эль-Гамаль, ГОСТ Р 34.10-94
5. Эль-Гамаль, DSA
6. DSA, ГОСТ Р 34.10-94
7. RSA, Эль-Гамаль
8. RSA, ГОСТ Р 34.10-94
9. RSA, DSA
10. Эль-Гамаль, DSA
11. Эль-Гамаль, ГОСТ Р 34.10-94
12. DSA, ГОСТ Р 34.10-94
13. RSA, DSA
14. RSA, ГОСТ Р 34.10-94
15. RSA, Эль-Гамаль
16. Эль-Гамаль, ГОСТ Р 34.10-94
17. Эль-Гамаль, DSA
18. DSA, ГОСТ Р 34.10-94
19. RSA, Эль-Гамаль
20. RSA, ГОСТ Р 34.10-94

21. RSA, DSA

Практическая часть

Вариант - 13. Номер варианта простых чисел. Число (41)

Второе число - 13 + 5 = 18. Число (61)

Метод RSA

p = 41 – составные части открытого ключа

q = 61 – составные части открытого ключа

n = 61 * 41 = 2501

φ(n) = 40 * 60 = 2400

e = 1

k = 11

Закрытый ключ $d^1 = 1 + 11 * 2400$; $d^1 = 26\,401$

Сообщение M = Николай передает привет. ; m = 22;

Цифровая подпись S = 22 * 26 401 (mod n) = 590.

Ответ: (m = 22; S = 590).

Метод DSA

G = 41

P = 61

q = 6

X = 4 – закрытый ключ

Y = 41 * 4 (mod 61) = 42 – открытый ключ

m = 4

K = 2

r = (1681 mod 61) mod 6 = 5

s = ((4 + 4 * 4)/2) mod 6 = 4

0 < r < q; 0 < s < q.

Условия выполняются

w = ((1/2) * (4 + 4 * 4)) mod 6 = 4

U1 = (4*4) mod 6 = 4

U2 = (4*4) mod 6 = 4

v = (((164 * 168) mod 61) mod 6 = 5

v = r

Вывод:

Была произведена генерация электронной цифровой подписи в соответствии с методами шифрования RSA и DSA. Вариант 1.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

МЕТОДЫ ОЦЕНКИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Тема:1,2 ,3,4	УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.	УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.
2	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.	Тема:2,4	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1 ПК-3	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
УК-1 ПК-3	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность

			подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1; ПК-3	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***ком петенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***ком петенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
11. Информационная безопасность при составление и направление ЭД участником – отправителем.
12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Примерная тематика заданий на контрольную работу:

1. Информационная безопасность модели Интернет - банкинга.
2. Информационная безопасность расчетов банковскими картами в Интернете.

3. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.

4. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.

5. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

6. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.

7. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

8. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.

9. Информационная безопасность электронных платежуй с помощью цифровых денег.

10. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.

11. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.

12. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

13. Информационная безопасность при составление и направление ЭД участником – отправителем.

14. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

15. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Методы оценки криптографической защиты информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	***Вид оценочного средства***	***Код компетенций, оценивающий знания, умения, навыки***	***Содержание оценочного средства***	***Требования к выполнению***	***Срок сдачи (неделя семестра)***	***Критерии оценки по содержанию и качеству с указанием баллов***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1 ПК-3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением.***

						Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%
Проводится в сроки, установленные графиком образовательного процесса	Экзамен	УК-1 ПК-3	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 20 минут на каждого студента	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных

						научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетво ри-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не

						отвечает на вопросы

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

4.1. Типовые вопросы, выносимые на экзамен (тестирование)

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

Вариант № 1

1. Как называтеся наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография

•Криптостойкость
•Криптометодология

2. Криптология включает в себя:
•Криптоанализ
•Криптография
•Криптосервис
•Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
•симметричным системам шифрования
•асимметричным системам шифрования
•однаключевым системам шифрования
•ключным системам

4. Простейшим из шифров замены является:
•одноалфавитная подставновка
•многоалфавитная замена
•гомофонический шифр
•малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?
•4
•3
•40
•7

6. Для наивной криптографии (до начала XVI в.) характерно использование:
•любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
•формализованных и относительно стойких к ручному криптоанализу шифров
•криптосистем со строгим математическим обоснованием криптостойкости
•вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

•с 1970-х гг.
•с 1980-х гг.
•с 1990-х гг.
•с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
•дейтаграммный
•виртуальный
•параллельный
•перпендикулярный

9. Сколько уровней в этолонной модели OSI?
•1
•13
•10
•7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
•2000
•1967
•1998
•2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
•да
•нет
•для государственных учреждений нет, а для комерческих предприятий да
•только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
•канальный
•представления
•прикладной

•сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

•ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”

•ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”

•ГОСТ Р ИСО\МЭК 15408

•Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

•предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств

•предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи

•предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации

•развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

•закрытие всех интернет-кафе

•лицензирование деятельности организаций в области защиты информации

•сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи

•введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 2

1. Как называтеся наука о способах преобразования информации с

целью ее защиты от незаконных пользователей?

- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:

- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- однаключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подставновка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем

"ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в этолонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для комерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

•канальный
•представления
•прикладной
•сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?
•ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
•ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
•ГОСТ Р ИСО\МЭК 15408
•Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

•предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
•предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
•предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
•развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:
•закрытие всех интернет-кафе
•лицензирование деятельности организаций в области защиты информации
•сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
•введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 3

1. Как называтся наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

•Криптология
•Криптография
•Криптостойкость
•Криптометодология

2. Криптология включает в себя:

•Криптоанализ
•Криптография
•Криптосервис
•Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

•симметричным системам шифрования
•асимметричным системам шифрования
•однаключевым системам шифрования
•ключным системам

4. Простейшим из шифров замены является:

•одноалфавитная подставновка
•многоалфавитная замена
•гомофонический шифр
•малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

•4
•3
•40
•7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

•любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
•формализованных и относительно стойких к ручному криптоанализу шифров
•криптосистем со строгим математическим обоснованием

криптостойкости

•вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

•с 1970-х гг.

•с 1980-х гг.

•с 1990-х гг.

•с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

•дейтаграммный

•виртуальный

•параллельный

•перпендикулярный

9. Сколько уровней в этолонной модели OSI?

•1

•13

•10

•7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

•2000

•1967

•1998

•2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

•да

•нет

•для государственных учреждений нет, а для комерческих предприятий да

•только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи

•введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

1.2. Типовые вопросы, выносимые на экзамен

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Классификация методов криптографического закрытия информации
5. Классические шифры.
6. Шифры гаммирования и колонной замены.
7. Простейшие шифры и их свойства.
8. Композиции шифров.
9. Системы шифрования с открытыми ключами.
10. Криптографическая стойкость шифров.
11. Модели шифров.
12. Основные требования к шифрам.
13. Вопросы практической стойкости.
14. Имитостойкость и помехоустойчивость шифров.
15. Принципы построения криптографических алгоритмов
16. Аппаратные средства. Программные средства, программные реализации шифров.
17. Крипто сервис провайдеры (CSP).
18. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи; ключевые системы.
19. Виртуальные частные сети.
20. Скремблеры.
21. Криптографические параметры узлов и блоков шифраторов.
22. Синтез шифров.
23. Методы получения случайных и псевдослучайных последовательностей.
24. Электронные цифровые подписи (электронные подписи).
25. Криптографические хеш-функции.
26. Криптографические протоколы.
27. Основные подходы к реализации PKI.
28. Компоненты и сервисы инфраструктуры открытых ключей.
29. Архитектура и топология PKI.
30. Стандарты в области PKI 50.
31. Стандарты Internet X.509 PKI (PKIX).
32. Сертификаты открытых ключей X.509.
33. Списки аннулированных сертификатов. Атрибутные

сертификаты.

34. Основные требования к политике PKI.
35. Политика применения сертификатов и регламент.
36. Краткая характеристика политики PKI.
37. Набор положений политики PKI.
38. Проблемы формирования политики PKI.
39. Симметричные криптосистемы.
40. Основы теории К. Шеннона.
41. Симметричные методы шифрования.
42. Алгоритмы блочного шифрования.
43. Режимы применения блочных шифров.
44. Потоковые шифры.
45. Комбинированные методы.
46. Односторонние функции и функции ловушки.
47. Асимметричные системы шифрования.
48. Применение асимметричных алгоритмов.
49. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
50. Хранилище сертификатов ОС MS Windows.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

МЕТОДЫ ОЦЕНКИ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

- Сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.
- Освоение студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

Задачи дисциплины:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

2. Указания по проведению практических занятий

Раздел 1. Основы информационной безопасности региона

Тема 1. Общие принципы информационной безопасности. Услуги безопасности. Угрозы. Механизмы

Практическое занятие 1.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.

2. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

3. Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Продолжительность занятия – 6 часов.

Тема 2. Теоретические основы криптографии. Криптографические методы защиты информации. Общие принципы и модели. Симметричные криптосистемы и блочные шифры. Асимметричные криптосистемы. Хэш-функции

Практическое занятие 2.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических методов защиты информации.

Основные положения темы занятия:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

2. Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89.

Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

3. Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамаля. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

4. Свойства хэш-функци. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHS, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Продолжительность занятия – 6 часов.

Раздел 2. Оценка криптографических методов систем защиты информации

Тема 3. Криптографические протоколы. Базовые принципы. Финансовая криптография. Электронные аукционы. Квантовая криптография. Биометрия Практическое занятие 3.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

Основные положения темы занятия:

- базовые протоколы криптографической защиты информации.
- квантовая криптография.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Принципы проектирования криптографических протоколов по Нидхему-Шредеру. Протокол «запрос-ответ».

2. Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.

3. Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

4. Принципы квантовой криптографии. Квантовый протокол распределения ключей.

5. Обзор биометрических методов. Метод биометрической «вуали».

Продолжительность занятия – 6 часов.

Тема 4. Управление ключами. Общие принципы. Депонирование ключей. Предварительное распределение ключей. Инфраструктура открытых ключей. Назначение PKI. Основные понятия. Принципы взаимодействия с УЦ. Список отозванных сертификатов

Практическое занятие 4.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: *практическая работа в группах*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки управления ключами.

Основные положения темы занятия:

- Управление ключами.
- Взаимодействие с УЦ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. пределения ключей Baffine.

2. Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSYD. Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).

3. Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (COC), приостановление действия сертификата,

Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура PKI. Понятие сертификационного пути. Преимущества PKI.

4. Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Продолжительность занятия – 6 часов.

3. Указания по проведению лабораторных работ

Не предусмотрены учебным планом

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Общие принципы информационной безопасности. Услуги безопасности. Угрозы. Механизмы	***Подготовка докладов по темам:*** Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента» Информационная безопасность модели Интернет - банкинга. Информационная безопасность расчетов банковскими картами в Интернете. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2.	Теоретические основы криптографии. Криптографические методы защиты информации. Общие принципы и модели. Симметричные криптосистемы и блочные шифры. Асимметричные криптосистемы. Хэш-функции	***Подготовка докладов по темам:*** Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП. Схема защищенного информационного обмена при использовании симметричных методов защиты информации. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3.	Криптографические протоколы. Базовые	***Подготовка докладов по темам:*** Применение и информационная

	принципы. Финансовая криптография. Электронные аукционы. Квантовая криптография. Биометрия	безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
	Управление ключами. Общие принципы. Депонирование ключей. Предварительное распределение ключей. Инфраструктура открытых ключей. Назначение PKI. Основные понятия. Принципы взаимодействия с УЦ. Список отозванных сертификатов	***Подготовка докладов по темам:*** Алгоритмы блочного шифрования. Асимметричные системы шифрования. Применение асимметричных алгоритмов. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – **…** страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Моделирование компьютерных сетей в среде NetCracker Professional 4.1 : методические указания / В. В. Пугин, И. С. Макаров, Е.

Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182305 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1.Электронные ресурсы образовательной среды Университета.

2.Информационно-справочная система (Консультант+; Гарант)