Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.О.27

Методы и средства криптографической защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 48
самостоятельная работа 59,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Контактная работа на аттестации	0,2	0,2	0,2	0,2
В том числе в форме практ.подготовки	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	59,8	59,8	59,8	59,8
Итого	108	108	108	108

Программу составил(и):
к.ф-м.н., доцент, Бужан Виталий Викорович

Рецензент(ы):
д.т.н., профессор кафедры информационных систем и программирования КубГТУ, Видовский Л.А.;д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.

Рабочая программа дисциплины
Методы и средства криптографической защиты информации

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

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины «Методы и средства криптографической защиты
1.2	информации» является изложение основополагающих принципов защиты информации с
1.3	помощью криптографических методов и средств, а также примеров реализации этих
1.4	методов на практике.
Задачи: Задачи дисциплины - дать основы: системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы информационной безопасности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Сети и телекоммуникации
2.2.2	Безопасность компьютерных сетей
2.2.3	Защита информации от утечки по техническим каналам
2.2.4	Учебная практика: Учебно-лабораторная практика
2.2.5	Производственная практика: Технологическая практика
2.2.6	Выполнение и защита выпускной квалификационной работы
2.2.7	Производственная практика: Преддипломная практика
2.2.8	Производственная практика: Эксплуатационная практика

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний использования средств криптографической защиты информации в автоматизированных системах
Уровень 2	Уровень знаний использования средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний использования средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	
Уметь	
Уровень 1	Продемонстрированы основные умения решения задач криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения решения задач криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения решения задач криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации	
Владеть	
Уровень 1	Имеется минимальный набор навыков организации защиты информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки организации защиты информации от утечки по техническим каналам на объектах информатизации с некоторыми недочётами

Уровень 3	Продемонстрированы навыки организации защиты информации от утечки по техническим каналам на объектах информатизации без ошибок и недочётов
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Оценивает угрозы информационной безопасности объекта информатизации
Уровень 2	Уровень знаний Оценивает угрозы информационной безопасности объекта информатизации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Оценивает угрозы информационной безопасности объекта информатизации в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения оценки угрозы информационной безопасности объекта информатизации , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценки угрозы информационной безопасности объекта информатизации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценки угрозы информационной безопасности объекта информатизации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Оценивает угрозы информационной безопасности объекта информатизации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Оценивает угрозы информационной безопасности объекта информатизации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Оценивает угрозы информационной безопасности объекта информатизации без ошибок и недочётов
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
Уровень 2	Уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Введение в криптографию					

1.1	Основные понятия, термины, определения. Криптология, криптография, криптоанализ /Лек/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
1.2	Основные задачи криптографии. Обеспечение конфиденциальности информации. Обеспечение целостности данных. Обеспечение доступности информации для всех авторизованных (законных) пользователей. /Ср/	4	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
1.3	Основные причины использования криптосистем. /Лаб/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1
1.4	Симметричная криптосистема. Криптосистема с открытым ключом. /Ср/	4	6,2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
1.5	Исторические шифры. Шифр сдвига. Полиалфавитный шифр. Шифр Виженера. Шифр Вернама. Недостатки исторических шифров. /Лаб/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1
1.6	Шифр замены. Частотный анализ. /Ср/	4	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Симметричные криптосистемы					
2.1	Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры /Лек/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
2.2	Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор ключевой последовательности, основанный на использовании алгебраических свойств М-последовательностей. Генератор псевдослучайных чисел, основанный на методе вычетов. Статистические тесты генераторов ключевого потока. Частотный тест. Сериальный тест. Покер тест. Корреляционный тест /Ср/	4	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Криптографические системы с открытым ключом					
3.1	Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма. /Лек/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
3.2	Задача криптоаналика. Криптостойкость RSA /Лаб/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1

3.3	Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование. /Ср/	4	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
3.4	Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование. /Лаб/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1
3.5	Простые числа. Важность проблемы тестирования простых чисел. Пробное деление. Вероятностный подход при определении простого числа. Тест Ферма. Тест Миллера - Рабина. /Ср/	4	8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
3.6	Схемы цифровой подписи: 1) RSA, 2) DSA /Лаб/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1
3.7	Хэш-функция /Ср/	4	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. Криптографические системы, основанные на физических механизмах защиты информации.					
4.1	Криптографическая Хэш-функция. Свойства криптографической хэш-функции. Свойство односторонности. /Лек/	4	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
4.2	Защищенность от повторений. Свойства криптографической хэш-функции. Защищенность от вторых прообразов. Алгоритмом цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. /Лаб/	4	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	2
4.3	Современные физические методы передачи секретных ключей. Основные требования к каналу связи. Метеорная криптография. Основные характеристики. Современные физические методы передачи секретных ключей. /Ср/	4	10	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	
4.4	Основные требования к каналу связи. Мобильная криптография. Основные характеристики /Лаб/	4	6	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	1
	Раздел 5. Промежуточная аттестация					
5.1	Зачет /КА/	4	0,2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Детерминированная модель открытого текста.
2. Вероятностные модели открытого текста: модель независимых символов алфавита, модель независимых биграмм, модель марковски зависимых букв.

3. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.
4. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.
5. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.
6. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.
7. Многоалфавитные шифры замены: табличное гаммирование, модульное гаммирование. Шифр Вернама.
8. Многоалфавитные шифры замены. Шифр пропорциональной замены (шифр омофонов).
9. Алгебраическая и вероятностная модели шифров.
10. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр, шифр замены с конечным ключом, шифр Виженера, шифр перестановки.
11. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.
12. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона.
13. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей.
14. (k|y)-совершенные шифры: определение, эквивалентные условия.
15. Необходимые и достаточные условия (k|y)-совершенных шифров.
16. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров.
17. Понятие опорного шифра, степени опорного шифра. Случайный и детерминированный генераторы ключевого потока. Примеры генераторов.
18. Определение шифра замены с ограниченным и неограниченным ключом.
19. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом.
20. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом.
21. Понятие имитации сообщений. Определение вероятности Рим. Нижняя оценка для вероятности имитации сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой имитации сообщений.
22. Понятие подмены сообщений. Определение вероятности Рподм. Нижняя оценка для вероятности подмены сообщения. Критерий достижимости нижней оценки. Примеры шифров с достижимой нижней оценкой подмены сообщений.
23. Совершенные имитостойкие шифры замены с неограниченным ключом.
24. Шифры, не распространяющие искажений типа замены знаков: определение, эквивалентные условия.
25. Понятие изометрии. Свойства изометрий.
26. Теорема А.А.Маркова. Примеры шифров, не распространяющих искажения типа замены знаков.
27. Шифры, не распространяющие искажений типа пропуска знаков: основные понятия.
28. Критерий для шифров, не распространяющеих искажений типа пропуска знаков, в классе эндоморфных шифров.
29. Шифры, не распространяющие искажений типа вставки знаков
30. Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ.
31. Схема разделения секрета Шамира.
32. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.
33. Схема разделения секрета на основе китайской теоремы об остатках.
34. Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера.
35. Схема Ито-Саито-Нишизеки.
36. Итеративные блочные шифры. Обратимость итеративного блочного шифра.
37. Шифры Фейстеля и их обратимость.
38. Построение цикловой функции. Входное и выходное отображения.
39. Слабые ключи итеративного блочного шифра.
40. Режимы использования симметричных блочных шифров.
41. Шифр Магма из ГОСТ Р 34.12-2015.
42. Криптоанализ симметричных блочных шифров.
43. Алгоритм быстрого возведения в степень. Задачи, приводящие к криптографии с открытым ключом и их решение.
44. Схема Диффи-Хеллмана.
45. Криптосистема без передачи ключа (шифр Шамира).
46. Шифр Эль-Гамаля.
47. Шифр RSA.
48. Рюкзачные криптосистемы.

5.2. Темы письменных работ

1. Применение алгоритма ГОСТ Р34.11-2012 для хэширования ключевой информации.
2. Разработка диспетчера доступа для типовой информационной системы.
3. Разработка диспетчера доступа для реляционных СУБД.
4. Аутентификация ОС МСВС.
5. Разработка системы аутентификации Windows для типового предприятия.
6. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в изображении.
7. Разработка стеганографической подсистемы защиты информации предприятия на основе методов скрытия информации в аудиофайлах.

8. Разработка подсистемы разграничения доступа СУБД предприятия.
9. Разработка подсистемы защиты электронного документооборота предприятия.
10. Разработка подсистемы разграничения доступа к информации на основе модели Харрисона-Руззо-Ульмана.
11. Разработка подсистемы защиты сайта от SQL-инъекции.
12. Разработка системы аутентификации для информационной системы типового предприятия.
13. Безопасность обработки данных облачными сервисами.
14. Модель администрирования ролевого управления доступом предприятия.

5.3. Фонд оценочных средств

1. Что такое шифрование?
а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
в) удобная среда для вычисления конечного пользователя

2. Что такое кодирование?
а) преобразование обычного, понятного текста в код
б) преобразование
в) написание программы

3. Для восстановления защитного текста требуется:
а) ключ
б) матрица
в) вектор

4. Сколько лет назад появилось шифрование?
а) четыре тысячи лет назад
б) две тысячи лет назад
в) пять тысяч лет назад

5. Первое известное применение шифра:
а) египетский текст
б) русский
в) нет правильного ответа

6. Секретная информация, которая хранится в Windows:
а) пароли для доступа к сетевым ресурсам
б) пароли для доступа в Интернет
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

7. Что такое алфавит?
а) конечное множество используемых для кодирования информации знаков
б) буквы текста
в) нет правильного ответа

8. Что такое текст?
а) упорядоченный набор из элементов алфавита
б) конечное множество используемых для кодирования информации знаков
в) все правильные

9. Выберите примеры алфавитов:
а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8
б) восьмеричный и шестнадцатеричный алфавиты
в) AEE

10. Что такое шифрование?
а) преобразовательный процесс исходного текста в зашифрованный
б) упорядоченный набор из элементов алфавита
в) нет правильного ответа

11. Что такое дешифрование?
а) на основе ключа шифрованный текст преобразуется в исходный
б) пароли для доступа к сетевым ресурсам
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Что представляет собой криптографическая система?
а) семейство T преобразований открытого текста, члены его семейства индексируются символом k
б) программу
в) систему

13. Что такое пространство ключей k?
а) набор возможных значений ключа
б) длина ключа
в) нет правильного ответа

14. На какие виды подразделяют криптосистемы?
а) симметричные
б) ассиметричные
в) с открытым ключом

15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
а) 1
б) 2
в) 3

16. Количество используемых ключей в системах с открытым ключом:
а) 2
б) 3
в) 1

17. Ключи, используемые в системах с открытым ключом:
а) открытый
б) закрытый
в) нет правильного ответа

18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
а) математически
б) логически
в) алгоритмически

19. Что принято называть электронной подписью?
а) присоединяемое к тексту его криптографическое преобразование
б) текст
в) зашифрованный текст

20. Что такое криптостойкость?
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
б) свойство гаммы
в) все ответы верны

21. Выберите то, что относится к показателям криптостойкости:
а) количество всех возможных ключей
б) среднее время, необходимое для криптоанализа
в) количество символов в ключе

22. Требования, предъявляемые к современным криптографическим системам защиты информации:
а) знание алгоритма шифрования не должно влиять на надежность защиты
б) структурные элементы алгоритма шифрования должны быть неизменными
в) не должно быть простых и легко устанавливаемых зависимостью между ключами +последовательно используемыми в процессе шифрования

23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
а) длина шифрованного текста должна быть равной лине исходного текста
б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
в) нет правильного ответа

24. Основными современными методами шифрования являются:
а) алгоритм гаммирования
б) алгоритмы сложных математических преобразований
в) алгоритм перестановки

25. Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
а) алгоритмом гаммирования
б) алгоритмом перестановки
в) алгоритмом аналитических преобразований

26. Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?
а) алгоритм перестановки
б) алгоритм подстановки
в) алгоритм гаммирования

27. Самая простая разновидность подстановки:
а) простая замена
б) перестановка
в) простая перестановка

28. Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
а) 3
б) 4
в) 5

29. Таблицы Вижинера, применяемые для повышения стойкости шифрования:
а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
б) в качестве ключа используется случайность последовательных чисел
в) нет правильного ответа

30. Суть метода перестановки:
а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
б) замена алфавита
в) все правильные

31. Цель криптоанализа:
а) Определение стойкости алгоритма
б) Увеличение количества функций замещения в криптографическом алгоритме
в) Уменьшение количества функций подстановок в криптографическом алгоритме
г) Определение использованных перестановок

32. По какой причине произойдет рост частоты применения брутфорс-атак?
а) Возросло используемое в алгоритмах количество перестановок и замещений
б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
в) Мощность и скорость работы процессоров возросла
г) Длина ключа со временем уменьшилась

33. Не будет являться свойством или характеристикой односторонней функции хэширования:
а) Она преобразует сообщение произвольной длины в значение фиксированной длины
б) Имея значение дайджеста сообщения, невозможно получить само сообщение
в) Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
г) Она преобразует сообщение фиксированной длины в значение переменной длины

34. Выберите то, что указывает на изменение сообщения:
а) Изменился открытый ключ
б) Изменился закрытый ключ
в) Изменился дайджест сообщения
г) Сообщение было правильно зашифровано

35. Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
а) Data Encryption Algorithm
б) Digital Signature Standard
в) Secure Hash Algorithm
г) Data Signature Algorithm

36. Выберите то, что лучше описывает отличия между HMAC и CBC-MAC?
а) HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
б) HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
в) HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC
г) HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

37. Определите преимущество RSA над DSA?
а) Он может обеспечить функциональность цифровой подписи и шифрования

б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи
в) Это блочный шифр и он лучше поточного
г) Он использует одноразовые шифровальные блокноты

38. С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
а) Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
б) Эти системы могут использоваться некоторыми странами против их местного населения
в) Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования
г) Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

39. Выберите то, что используют для создания цифровой подписи:
а) Закрытый ключ получателя
б) Открытый ключ отправителя
в) Закрытый ключ отправителя
г) Открытый ключ получателя

40. Выберите то, что лучше всего описывает цифровую подпись:
а) Это метод переноса собственноручной подписи на электронный документ
б) Это метод шифрования конфиденциальной информации
в) Это метод, обеспечивающий электронную подпись и шифрование
г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Москвитин Г. И.	Комплексная защита информации в организации: Монография	Москва: Русайнс, 2020, URL: https://book.ru/book/934814
Л1.2	Московский государственный технический университет гражданской авиации	Информационный мир XXI века. Криптография- основа информационной безопасности: Учебно-методическая литература	Москва: Издательско-торговая корпорация "Дашков и К", 2020, URL: https://znanium.com/catalog/document?id=353538
Л1.3	Фомичев В.М.	Криптография — наука о тайнописи: Учебное пособие	Москва: Прометей, 2020, URL: https://znanium.com/catalog/document?id=389799

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2019, URL: https://book.ru/book/932909
Л2.2	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020, URL: http://znanium.com/catalog/document?id=358722
Л2.3	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=361143
Л2.4	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021, URL: http://znanium.com/catalog/document?id=364911

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	Национальный открытый университет "ИНТУИТ" . - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Электронно-библиотечная система . - Режим доступа: http://znanium.com/%20
Э3	ЭИОС. - Режим доступа: http://eios.imsit.ru/
Э4	ЭБС Айбукс. - Режим доступа: http://www.ibooks.ru/

Э5	РПД. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
114а	Лаборатория программно-аппаратных средств защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
123	Кабинет информационной безопасности	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт.,

		LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	проекционный экран – 1 шт., соответствующее программное обеспечение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.

Учебный материал по дисциплине «Методы и средства криптографической защиты информации», разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.

Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только

знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Методы и средства криптографической защиты информации».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями