

Федеральное государственное образовательное бюджетное учреждение  
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ  
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»  
(Финансовый университет)**

**АЛТАЙСКИЙ ФИЛИАЛ**

**Кафедра «Учет и информационные технологии в бизнесе»**

**Разработчик: Е.К. Баранова**

**Составитель: О.Г. Солодкий**

**Основы криптографии**

Рабочая программа дисциплины  
для студентов, обучающихся по направлению подготовки  
09.03.03 «Прикладная информатика»

**Барнаул, 2022**


Федеральное государственное образовательное бюджетное учреждение  
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ  
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»  
(Финансовый университет)  
АЛТАЙСКИЙ ФИЛИАЛ**

**Кафедра «Учет и информационные технологии в бизнесе»**

УТВЕРЖДАЮ

Директор филиала

 Иванова В.А.

«26» апреля 2022 г.

**Разработчик: Е.К. Баранова**

**Составитель: О.Г. Солодкий**

**Основы криптографии**

Рабочая программа дисциплины  
для студентов, обучающихся по направлению подготовки  
09.03.03 «Прикладная информатика»

*Рекомендовано Ученым Советом Алтайского филиала*

*(протокол №48 от «26» апреля 2022 г.)*

*Одобрено кафедрой «Учет и информационные технологии в бизнесе»*

*(протокол №9 от «31» марта 2022 г.)*

**Барнаул 2022**

## СОДЕРЖАНИЕ

1. Наименование дисциплины.....	4
2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине.....	4
3. Место дисциплины в структуре образовательной программы.....	7
4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся.....	7
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий.....	7
5.1 Содержание тем дисциплины.....	7
5.2 Учебно-тематический план.....	9
5.3 Содержание семинаров, практических занятий.....	11
6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине.....	14
6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	14
6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю.....	15
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	18
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	30
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	31
10. Методические указания для обучающихся по освоению дисциплины.....	31
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем.....	31
12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.....	32

## 1. Наименование дисциплины

«Основы криптографии».

## 2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1. Использует информационно-коммуникационные технологии и библиографические источники при поиске информации, для решения стандартных задач.	<b>Знать</b> основные способы сбора, обработки и анализа научно-технической информации по обеспечению конфиденциальности и целостности данных в информационно-телекоммуникационных системах. <b>Уметь</b> на практике применять способы сбора, обработки и анализа научно-технической информации по обеспечению конфиденциальности и целостности данных в информационно-телекоммуникационных системах.
		2. Демонстрирует умение решать стандартные задачи разработки информационных систем.	<b>Знать</b> основные стандартные алгоритмы защиты информации и способы их применения. <b>Уметь</b> составлять планы и программы научных исследований и технических разработок в области защиты данных в информационно-телекоммуникационных системах.
		3. Владеет навыками обеспечения информационной безопасности автоматизированных систем.	<b>Знать</b> основные направления в сфере обеспечения защиты данных финансового сектора. <b>Уметь</b> организовывать процессы по прогнозированию и учету основных направлений развития в сфере обеспечения защиты данных финансового сектора.

ПКН-7	Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения, в том числе с учетом требований информационной безопасности	<p>1. Демонстрирует знание основ функционирования компьютерной техники, решает часто возникающие проблемы в их эксплуатации, выполняет первичную установку и настройку популярных программ и операционных систем.</p> <p>2. Демонстрирует знание основ функционирования операционных систем и компьютерных сетей, настраивает сетевые подключения и службы, диагностирует их работу и решает типичные задачи администрирования сетей.</p> <p>3. Использует серверные операционные системы для разработки и развертывания сетевых приложений, настраивает веб-службы, частично автоматизирует эти процессы.</p> <p>4. Демонстрирует знание основ компьютерной безопасности,</p>	<p><b>Знать</b> основы функционирования компьютерной техники и возникающие проблемы в их эксплуатации.</p> <p><b>Уметь</b> выполнять первичную установку и настройку популярных программ и операционных систем с учетом требований информационной безопасности.</p> <p><b>Знать</b> основы функционирования операционных систем и компьютерных сетей с учетом требований информационной безопасности.</p> <p><b>Уметь</b> решать типовые задачи администрирования сетей с учетом требований по шифрованию данных.</p> <p><b>Знать</b> основы функционирования серверных операционных систем для разработки и развертывания сетевых приложений, с учетом требований информационной безопасности.</p> <p><b>Уметь</b> развертывать сетевые приложения, и обеспечивать настройку веб-приложений с учетом требований по шифрованию данных.</p> <p><b>Знать</b> основы компьютерной безопасности информационно-телекоммуникационных сетей.</p> <p><b>Уметь</b> использовать современные алгоритмы шифрования, хеширования,</p>
-------	--	--	---

		<p>алгоритмов шифрования, хеширования, понятий аутентификации, авторизации, цифровых сертификатов, протоколов безопасной передачи данных.</p>	<p>идентификации и аутентификации.</p>
ПКН-2	<p>Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования (ПКН-2)</p>	<p>1. Владеет объектно-ориентированным языком программирования на уровне знания синтаксиса и семантики, основ стандартной библиотеки.</p> <p>2. Использует инструментальные средства программирования (IDE, SDK, API, популярные фреймворки и библиотеки).</p>	<p><b>Знать</b> основы современных объектно-ориентированных языков программирования.</p> <p><b>Уметь</b> использовать современные технологий программирования и стандартные библиотеки.</p> <p><b>Знать</b> современные инструментальные средства программирования.</p> <p><b>Уметь</b> использовать популярные фреймворки и стандартные библиотеки для достижения высокой скорости разработки проектов по обеспечению безопасности данных.</p>

		3. Организует кодовую базу, ориентируется в существующем коде, демонстрирует знание общепринятых соглашений и политик в области оформления кода.	<b>Знать</b> принципы организации кодовой базы.  <b>Уметь</b> ориентироваться в существующем коде, и демонстрировать знание общепринятых соглашений и политик безопасности в области оформления кода.
--	--	--	---

		4. Проектирует текстовый, программный или графический интерфейс программной системы исходя из ее назначения.	<b>Знать</b> принципы проектирования программного и графического интерфейса программной системы с учетом требований информационной безопасности.  <b>Уметь</b> настраивать программный или графический интерфейс системы исходя из ее назначения.
--	--	--	---

### 3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы криптографии» относится к общепрофессиональному циклу дисциплин.

### 4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 1

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 3/4 (в часах)
<b>Общая трудоемкость дисциплины</b>	4 з.е./144	144
<b>Контактная работа – Аудиторные занятия</b>	50/34/16	50/34/16

<i>Лекции</i>	16//16/4	16//16/4
<i>Семинары, практические занятия</i>	34/18//12	34/18//12
<b><i>Самостоятельная работа</i></b>	94/110/128	94/110/128
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Зачет	Зачет

## **5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий**

### **5.1 Содержание тем дисциплины**

#### **Тема 1. Общие понятия криптографической защиты информации**

Место криптографической защиты информации в обеспечении информационной безопасности. Краткие сведения из истории криптографии. Примеры реализации классических шифров моноалфавитных, многоалфавитных подстановок и шифров перестановки. Требования к системам шифрования и примеры их реализации в классических криптографических алгоритмах.

#### **Тема 2. Математические основы криптологии**

Алгебры: полугруппы и группы, кольца, поля, векторные пространства. Циклические группы, порядок элемента. Кольца матриц, многочленов, целых чисел, вычетов по модулю  $m$ . Операции над множествами. Отображение множеств. Мощность множеств. Отношения на множествах. Бинарные отношения на множествах: эквивалентность, частичный порядок, диаграммы. Дискретные функции, преобразования множеств, подстановки. Граф преобразования, подстановки.

Базовые определения криптографии: стойкость шифра; объем ключа; помехоустойчивость шифра; имитостойкость шифра; разрастание числа ошибок.

#### **Тема 3. Симметричные системы шифрования**

Перемешивающие свойства преобразований. Строение итеративных блочных шифров, SP-сети, сети Фейстеля. Раундовая функция, S-боксы, ключевое расписание. Базовый режим ECB, свойства, основные недостатки. Режимы CBC, OFB. Структурная схема симметричной криптосистемы. Обзор современных симметричных алгоритмов блочного шифрования. DES (Data Encryption Standard). Обобщенная схема шифрования. Реализация функции шифрования. Получение раундовых ключей. Оценка криптостойкости алгоритма DES. Режимы работы DES. Алгоритм Blowfish. Инициализация. Функция шифрования. Сравнение алгоритмов Blowfish и DES. Отечественный



стандарт симметричного шифрования: логика построения шифра; режимы работы. AES Rijndael: схема преобразования данных при шифровании. Схема раунда алгоритма Rijndael.  $S[]$  – функция подстановки байт для алгоритма Rijndael (S-блок). Получение раундовых ключей в алгоритме Rijndael. Сравнительные характеристики современных алгоритмов симметричного шифрования.

#### **Тема 4. Асимметричные системы шифрования**

Вычислительная сложность алгоритмов факторизации и дискретного логарифмирования. Простые и взаимно простые числа. Алгоритм Евклида и расширенный алгоритм Евклида. Арифметика остатков. Группы и кольца. Функция Эйлера. Малая теорема Ферма и теорема Эйлера. Решение сравнений в кольцах вычетов. Китайская теорема об остатках. Проверка чисел на простоту. Метод пробных делений. Решето Эратосфена. Вероятностный тест Ферма. Числа Кармайкла. Краткий обзор современных асимметричных систем шифрования. Обобщенная схема асимметричной системы шифрования. Алгоритм RSA (Rivest-Shamir-Adleman). Алгоритм Эль-Гамала (El Gamal).

#### **Тема 5. Электронная подпись**

Хэш-функции, определение и общие требования. Однонаправленные функции, хэш-функции, коллизии. Хэш-функции на основе блочного шифрования. Электронная подпись (ЭП): общие понятия и определения, требования и структура ЭП. Процедуры постановки и проверки подлинности ЭП. Схема формирования ЭП (на примере использования алгоритмов RSA и Эль-Гамала). Процедуры постановки и проверки ЭП ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Нормативно-правовое регулирование в области использования электронной подписи №63-ФЗ «Об электронной подписи». Основные требования к цифровым подписям, квалифицированная и неквалифицированная ЭП.

#### **Тема 6. Управление криптографическими ключами**

Ключи криптосистемы: размер, случайность, секретность. Виды ключей. Жизненный цикл ключей: генерация, распределение, хранение, смена, обновление, уничтожение. Алгоритм открытого распределения ключей Диффи-Хеллмана (Diffie-Hellman). Снабжение пользователей ключами в симметричных и асимметричных криптосистемах. Методы управления криптографическими ключами. Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17. Хранение криптографических

ключей. Иерархия криптографических ключей. Схема аутентификации мастер-ключа. Схема защиты сеансового ключа. Распределение криптографических ключей. Протоколы аутентификации и распределения ключей для симметричных криптосистем.

## **Тема 7. Перспективные направления в области криптографической и стеганографической защиты информации**

Проблемы стойкости криптографических систем. Современные приложения криптографии. Стеганографические методы защиты информации. Цифровые водяные знаки.

### **5.2 Учебно-тематический план (очная, очно-заочная, заочная форма обучения)**

Таблица 2

№ п/п	Наименование темы дисциплины	Трудоёмкость в часах					Формы текущего контроля успеваемости
		Всего часов	Аудиторная работа			Сам. раб.	
			Общая	Лекции	Семинары		
1.	Тема 1. Общие понятия криптографическо й защиты информации	16/22/23	4/4/1	2/2/0	2/2/1	12/18/22	Доклады, презентации, обсуждение в группе. Выступление или сообщение с презентацией, дискуссии, тематические опросы.
2.	Тема 2. Математические основы криптологии	24/24/28	8/4/4	2/2/2	6/2/2	16/20/24	Выступление или сообщение с презентацией, дискуссии, тематические опросы. Обсуждение в группе, опрос, решение задач.
3.	Тема 3. Симметричные системы шифрования	24/26/25	10/8/3	4/4/1	6/4/2	14/18/22	Выступление или сообщение с презентацией, дискуссии, тематические опросы. Групповые и индивидуальные практические задания.
4.	Тема 4.						Выступление или

	Асимметричные системы шифрования	22/22/23	8/6/3	2/2/1	6/4/2	14/16/20	сообщение с презентацией, дискуссии, тематические опросы. Групповые и индивидуальные практические задания
5.	Тема 5. Электронная подпись	22/18/17	8/4/1	2/2/0	6/2/1	14/14/16	Выступление или сообщение с презентацией, дискуссии, тематические опросы. Групповые и индивидуальные практические задания
6.	Тема 6. Управление криптографическими ключами	20/18/18	6/4/2	2/2/0	4/2/2	14/14/16	Выступление или сообщение с презентацией, дискуссии, тематические опросы. Групповые и индивидуальные практические задания
7.	Тема 7. Перспективные направления в области криптографической и стеганографической защиты информации	16/14/10	6/4/2	2/2/0	4/2/2	10/10/8	Доклады, презентации, обсуждение в группе. Выступление или сообщение с презентацией, дискуссии, тематические опросы
	В целом по дисциплине	144	50/34/16	16/16/4	34/18/12	94/110/128	Согласно учебному плану : контрольная работа
	Итого в %:		35%/27%/11%	32%/47%/25%	68%/53%/75%	65%/73%/89%	

### 5.3 Содержание семинаров, практических занятий

Таблица 3

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9 (указывается раздел и порядковый номер источника)	Формы проведения занятий
Тема 1. Общие понятия криптографической защиты информации	<p>Этапы истории криптографии. Классические криптографические алгоритмы: моноалфавитные подстановки. Классические криптографические алгоритмы: многоалфавитные подстановки. Классические криптографические алгоритмы: перестановки.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.2</p>	<p>Выступление или сообщение с презентацией, дискуссии, тематические опросы. Подготовка докладов с презентациями.</p> <p><i>Учебное задание:</i></p> <p>Исследование классических методов шифрования перестановки и замены. Частотный анализ исходных и зашифрованных текстов (источник 8.2, с.19)</p>
Тема 2. Математические основы криптологии	<p>Операции над множествами. Отображение множеств. Мощность множеств. Отношения на множествах. Бинарные отношения на множествах: эквивалентность, частичный порядок, диаграммы. Дискретные функции, преобразования множеств, подстановки. Граф преобразования, подстановки.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.3, 8.4</p>	<p>Выступление или сообщение с презентацией, дискуссии, тематические опросы.</p> <p><i>Учебное задание:</i></p> <p>Тестовое задание (источник 8.1, с.20). Решение задач (источник 8.1, с.180)</p>

Тема 3. Симметричные системы шифрования	<p>Сеть Фейстеля. Режимы работы DES. Алгоритм Blowfish: инициализация; функция шифрования. Сравнение алгоритмов Blowfish и DES. Отечественный стандарт симметричного шифрования: логика построения шифра; режимы работы. AES Rijndael: схема преобразования данных при шифровании. Схема раунда алгоритма Rijndael. S[] – функция подстановки байт для алгоритма Rijndael (S-блок). Получение раундовых ключей в алгоритме Rijndael.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.2</p>	<p>Дискуссии, тематические опросы. Подготовка докладов с презентациями. Тестирование.</p> <p><i>Учебное практическое задание:</i> Исследование работы сети Фейстеля (источник 8.2, с.116)</p>
Тема 4. Асимметричные системы шифрования	<p>Проверка чисел на простоту. Метод пробных делений. Решето Эратосфена. Вероятностный тест Ферма. Числа Кармайкла. Краткий обзор современных асимметричных систем шифрования. Обобщенная схема асимметричной</p>	<p>Выступление или сообщение с презентацией, дискуссии. Тестирование.</p> <p><i>Учебное практическое задание:</i> Методы генерации простых чисел, используемых в асимметричных системах шифрования. (источник 8.2, с.61)</p>
	<p>системы шифрования. Алгоритм RSA. Алгоритм Эль-Гамала.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.2</p>	

Тема 5. Электронная подпись	<p>Процедуры постановки и проверки ЭП ГОСТ 34.10-2018 «Информационная технология.</p> <p>Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Нормативно-правовое регулирование в области использования электронной подписи №63-ФЗ «Об электронной подписи». Основные требования к цифровым подписям, квалифицированная и неквалифицированная ЭП.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.2</p>	<p>Дискуссии, тематические опросы.</p> <p>Подготовка докладов с презентациями.</p> <p>Тестирование (<i>источник 8.1, с.174</i>)</p>
Тема 6. Управление криптографическими ключами	<p>Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17. Хранение криптографических ключей. Иерархия криптографических ключей. Схема аутентификации мастер-ключа. Схема защиты сеансового ключа. Распределение криптографических ключей.</p> <p><i>Рекомендуемые источники:</i> 8.1, 8.2</p>	<p>Дискуссии, тематические опросы.</p> <p>Подготовка докладов с презентациями.</p> <p>Тестирование (<i>источник 8.1, с.147</i>)</p>
Тема 7. Перспективные	Стеганографические методы защиты информации. Методы	Выступление или сообщение с презентацией, дискуссии.

направления в области криптографической и стеганографической защиты информации	встраивания данных в мультимедийные контейнеры. Использование цифровых водяных знаков для защиты авторских прав. Перспективы использования методов стеганографии для защиты цифрового контента – плюсы и минусы.  <i>Рекомендуемые источники:</i>  8.1, 8.2	<i>Учебное практическое задание:</i> Использования методов стеганографии для защиты цифрового контента. (источник 8.2, с.169)
--	---	---

## 6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

### 6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Общие понятия криптографической защиты информации	Шифрование информации методом гаммирования. Современные приложения криптографических методов защиты информации.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>
Тема 2. Математические основы криптологии	Программные реализации: проверка чисел на простоту; метод пробных делений; решето Эратосфена; числа Кармайкла.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>

Тема 3. Симметричные системы шифрования	AES Rijndael: схема преобразования данных при шифровании. Схема раунда алгоритма Rijndael. $S[]$ – функция подстановки байт для алгоритма Rijndael (S-блок). Получение раундовых ключей в алгоритме Rijndael.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>
---	---	---

Тема 4. Асимметричные системы шифрования	Обобщенная схема асимметричной системы шифрования. Алгоритм RSA. Алгоритм Эль-Гамала.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>
Тема 5. Электронная подпись	Нормативно-правовое регулирование в области использования электронной подписи №63-ФЗ «Об электронной подписи». Основные требования к цифровым подписям, квалифицированная и неквалифицированная ЭП.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>
Тема 6. Управление криптографическими ключами	Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>
Тема 7. Перспективные направления в области криптографической и стеганографической защиты информации	Использование цифровых водяных знаков для защиты авторских прав. Перспективы использования методов стеганографии для защиты цифрового контента – плюсы и минусы.	<ul style="list-style-type: none"> <li>- работа с учебной, научной и справочной литературой;</li> <li>- конспект;</li> <li>- подготовка докладов по теме;</li> <li>- подготовка презентаций по теме;</li> <li>- выполнение учебного задания.</li> </ul>

## 6.2. Перечень вопросов, заданий, тем для подготовки к



## текущему контролю

### *Основные формы текущего контроля (контрольная работа):*

- контрольная работа;
- подготовка докладов с презентациями по теме;
- выполнение текущих заданий по тематике учебных практических заданий.

### *Примерный перечень задач к контрольной работе*

**Задача 1.** Оценить вычислительную сложность определения закрытого ключа асимметричной криптосистемы RSA по открытому ключу заданной длины.

**Задача 2.** Оценить вычислительную сложность нахождения коллизии для ряда стандартных хэш-функций методом на основе парадокса дней рождения.

**Задача 3.** Оценить вычислительную сложность определения ключа симметричного блочного шифра с линейной раундовой подстановкой.

**Задача 4.** Определить длину периода и линейную сложность гаммы, генерируемой комбинирующим нелинейным генератором.

**Задача 5.** Оценить размер необходимой памяти и вычислительную сложность определения ключа симметричного блочного шифра методом согласования для случая независимых раундовых ключей.

**Задача 6.** Написать набор подпрограмм, реализующих базовые алгоритмы, используемые в изученных криптосистемах: возведение в степень по модулю ( $a^x \bmod m$ ), вычисление наибольшего общего делителя ( $\gcd(a, b)$ ), вычисление инверсии ( $x^{-1} \bmod m$ ).

**Задача 7.** Написать программу, реализующую схему открытого распространения ключей Диффи–Хеллмана. Рекомендуемые значения параметров  $p = 30803$ ,  $g = 2$ . Секретные ключи генерировать случайным образом.

**Задача 8.** Написать программу, реализующую алгоритм шифрования Шамира. В качестве простого модуля можно взять число  $p = 30803$ . Остальные параметры генерировать случайным образом.

**Задача 9.** Написать программу, реализующую алгоритм шифрования Эль-Гамала. Рекомендуемые значения параметров  $p = 30803$ ,  $g = 2$ . Секретные ключи и другие параметры генерировать случайным образом.

**Задача 10.** Написать программу, реализующую алгоритм шифрования RSA для передачи секретных сообщений в адрес абонентов А или В. Рекомендуемые значения параметров  $P_A = 131$ ,  $Q_A = 227$ ,  $P_B = 113$ ,  $Q_B = 281$ ,  $d_A = d_B = 3$ .

### *Примерный перечень докладов с презентациями*

1. Краткие сведения из истории криптографии.
2. Классификация классических криптоалгоритмов, примеры реализации моноалфавиных, многоалфавитных подстановок и шифров перестановок.
3. Методы замены. Примеры реализации моноалфавитной и

многоалфавитной замены.

4. Перестановочные шифры, шифры усложненной перестановки.
5. Шифрование с использованием методов аналитических преобразований.
6. Шифры гаммирования.
7. Структурная схема симметричной криптосистемы.
8. Сеть Фейстеля.
9. Обзор современных симметричных алгоритмов блочного шифрования.
10. DES (Data Encryption Standard). Обобщенная схема шифрования.
11. Области применения DES (Data Encryption Standard).
12. Симметричные криптографические системы. Алгоритм Blowfish.
13. Отечественный стандарт симметричного шифрования. Логика построения шифра.
14. Симметричные криптографические системы. AES Rijndael.
15. Сравнительные характеристики алгоритмов DES и AES Rijndael.
16. Обобщенная схема асимметричной системы шифрования. Общие понятия и определения.
17. Алгоритм открытого распределения ключей Диффи–Хеллмана (Diffie - Hellman).
18. Алгоритм RSA (Rivest-Shamir-Adleman).
19. Алгоритм Эль-Гамала (El Gamal).
20. Электронная подпись. Общие понятия и определения, требования и структура ЭП.
21. Процедуры постановки и проверки подлинности ЭП.
22. Хэш-функции: определение и общие требования.
23. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
24. Современные приложения криптографии.

### ***Примерный перечень тематики учебных практических заданий***

Классические криптосистемы. Этапы истории криптографии. Классические шифры: моноалфавитные подстановки; многоалфавитные подстановки; перестановки. Шифрование информации методом гаммирования.

Шифры усложненной перестановки и замены. Решение задач по использованию классических методов шифрования.

Математические основы криптологии. Программные реализации:

проверка чисел на простоту; метод пробных делений; решето Эратосфена; числа Кармайкла.

Современные симметричные системы шифрования. Алгоритм симметричного шифрования DES. Алгоритм симметричного шифрования IDEA. Алгоритм симметричного шифрования Rijndael. Алгоритм симметричного шифрования Blowfish. Отечественный стандарт симметричного шифрования.

Современные асимметричные системы шифрования. Алгоритм асимметричного шифрования RSA. Алгоритм асимметричного шифрования Эль-Гамала. Комбинированные методы шифрования.

Электронная подпись. Хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи DSA. Алгоритм цифровой подписи Эль-Гамала. Отечественный стандарт цифровой подписи.

Управление криптографическими ключами. Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17. Хранение криптографических ключей. Иерархия криптографических ключей. Схема аутентификации мастер-ключа. Схема защиты сеансового ключа. Распределение криптографических ключей. Протоколы аутентификации и распределения ключей для симметричных криптосистем.

Методы стеганографической защиты информации. Методы встраивания данных в мультимедийные контейнеры. Использование цифровых водяных знаков для защиты авторских прав. Перспективы использования методов стеганографии для защиты цифрового контента – плюсы и минусы.

В течение семестра студент может набрать максимальное количество баллов равное 40. На промежуточную аттестацию (зачет) отводится 60 баллов. Распределение баллов по видам работ, формирующих текущий контроль успеваемости по дисциплине, отражает качество подготовки обучающихся к занятиям семинарского типа и выполнение различных видов самостоятельной работы.

### ***Критерии балльной оценки различных форм текущего контроля***

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических

рекомендациях Департамента информационной безопасности.

## 7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, формируемых в процессе освоения дисциплины, содержится в разделе 2. Перечень планируемых результатов освоения образовательной программы с указанием индикаторов их достижения, соотнесенных с планируемыми результатами обучения по дисциплине.

### Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, знаний и умений

Таблица 5

Наименование компетенции	Наименование индикаторов достижения компетенции	Результаты обучения (умения и знания), соотнесенные и индикаторами достижения компетенций	Типовые контрольные задания
<b>ОПК-3</b> Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>Индикатор 1</b> Использует информационно-коммуникационные технологии и библиографические источники при поиске информации, для решения стандартных задач.	<b>Знать</b> основные способы сбора, обработки и анализа научно-технической информации по обеспечению конфиденциальности и целостности данных в информационно-телекоммуникационных системах. <b>Уметь</b> на практике применять способы сбора, обработки и анализа научно-технической информации по обеспечению конфиденциальности и целостности данных в информационно-телекоммуникационных	<b>Задание</b> Составить план внедрения в информационную систему организации наиболее эффективного ПО для контроля целостности данных.

	<p><b>Индикатор 2</b> Демонстрирует умение решать стандартные задачи разработки информационных систем.</p> <p><b>Индикатор 3</b> Владеет навыками обеспечения информационной безопасности автоматизированных систем.</p>	<p>системах. <b>Знать</b> основные стандартные алгоритмы защиты информации и способы их применения. <b>Уметь</b> составлять планы и программы научных исследований и технических разработок в области защиты данных в информационно-телекоммуникационных системах. <b>Знать</b> основные направления в сфере обеспечения защиты данных финансового сектора. <b>Уметь</b> организовывать процессы по прогнозированию и учету основных направлений развития в сфере обеспечения защиты данных финансового сектора.</p>	<p><b>Задание</b> Подготовить перечень криптографических средств для защиты от основных угроз информационной безопасности в информационной системе организации.</p> <p><b>Задание</b> Подготовить проект внутреннего нормативного документа в конкретной организации по работе с ключевой информацией (документацией) криптографических систем защиты информации.</p>
<p><b>ПКН-2</b> Способность разрабатывать алгоритмы и программы с использованием современных технологий программирования</p>	<p><b>Индикатор 1</b> Владеет объектно-ориентированным языком программирования на уровне знания синтаксиса и семантики, основ стандартной библиотеки.</p> <p><b>Индикатор 2</b></p>	<p><b>Знать</b> основы современных объектно-ориентированных языков программирования. <b>Уметь</b> использовать современные технологий программирования и стандартные библиотеки.</p> <p><b>Знать</b> современные</p>	<p><b>Задание</b> Подготовить программу для шифрования данных с использованием классических криптоалгоритмов.</p> <p><b>Задание</b> Написать программу, реализующую алгоритм Эль-</p>

	<p>Использует инструментальные средства программирования (IDE, SDK, API, популярные фреймворки и библиотеки)</p> <p><b>Индикатор 3</b> Организовывает кодовую базу, ориентируется в существующем коде, демонстрирует знание общепринятых соглашений и политик в области оформления кода.</p> <p><b>Индикатор 4</b> Проектирует текстовый, программный или графический интерфейс программной системы исходя из ее назначения.</p>	<p>инструментальные средства программирования. <b>Уметь</b> использовать популярные фреймворки и стандартные библиотеки для достижения высокой скорости разработки проектов по обеспечению безопасности данных.</p> <p><b>Знать</b> принципы организации кодовой базы. <b>Уметь</b> ориентироваться в существующем коде, и демонстрировать знание общепринятых соглашений и политик безопасности в области оформления кода.</p> <p><b>Знать</b> принципы проектирования программного или графического интерфейса программной системы с учетом требований информационной безопасности. <b>Уметь</b> настраивать программный или графический интерфейс системы исходя из ее назначения.</p>	<p>Гамалая. Рекомендуемые значения параметров <math>p = 30803</math> , <math>g = 2</math> .</p> <p><b>Задание</b> Описать политику безопасности, используемую в телекоммуникационной сети конкретной организации (проанализировать плюсы и минусы)</p> <p><b>Задание</b> Проанализировать работу VPN-сети конкретной организации, описать методы шифрования, используемые при передачи данных по туннелю.</p>
<p><b>ПКН-7</b> Способность выполнять сервисное обслуживание и настройку аппаратного и программного обеспечения, в том числе с учетом требований информационной безопасности</p>	<p><b>Индикатор 1</b> Демонстрирует знание основ функционирования компьютерной техники, решает часто возникающие проблемы в их эксплуатации, выполняет первичную установку и настройку популярных программ и операционных систем.</p>	<p><b>Знать</b> основы функционирования компьютерной техники и возникающие проблемы в их эксплуатации. <b>Уметь</b> выполнять первичную установку и настройку популярных программ и знаний информационной безопасности.</p>	<p><b>Задание</b> Проанализировать работу VPN-сети конкретной организации, описать методы шифрования, используемые при передачи данных по туннелю.</p>

			<b>Задание</b>
--	--	--	----------------

	<p><b>Индикатор 2</b> Демонстрирует знание основ функционирования операционных систем и компьютерных сетей, настраивает сетевые подключения и службы, диагностирует их работу и решает типичные задачи администрирования сетей.</p>	<p><b>Знать</b> основы функционирования операционных систем и компьютерных сетей с учетом требований информационной безопасности. <b>Уметь</b> решать типичные задачи администрирования сетей с учетом требований по шифрованию данных.</p>	<p>Управление журналом аудита безопасности конкретной организации (настройка параметров: локальной политики; политики сайта; политики домена; политики подразделения)</p>
	<p><b>Индикатор 3</b> Использует серверные операционные системы для разработки и развертывания сетевых приложений, настраивает веб-службы, частично автоматизирует эти процессы.</p> <p><b>Индикатор 4</b>  Демонстрирует знание основ компьютерной безопасности, алгоритмов шифрования, хеширования, понятий аутентификации, авторизации, цифровых сертификатов, протоколов безопасной передачи данных.</p>	<p><b>Знать</b> основы функционирования серверных операционных систем для разработки и развертывания сетевых приложений, с учетом требований информационной безопасности. <b>Уметь</b> развертывать сетевые приложения, и обеспечивать настройку веб-приложений с учетом требований по шифрованию данных.</p> <p><b>Знать</b> основы компьютерной безопасности информационно-телекоммуникационных сетей.  <b>Уметь</b> использовать современные алгоритмы шифрования, хеширования, идентификации и аутентификации.</p>	<p><b>Задание</b> Оценить безопасность веб-приложения конкретной организации с учетом основного бизнес-процесса.</p> <p><b>Задание</b> Оценить вычислительную сложность нахождения коллизии для ряда стандартных хеш-функций различными методами.</p>

## **Примеры теоретико-прикладных вопросов (тестовое задание)**

### ***Пример тестового задания***

#### **Тема 3. Симметричные системы шифрования**

- 1. Преобразование открытого текста сообщения в закрытый называется:**
  - 1) процедура шифрования;
  - 2) алгоритм шифрования;
  - 3) обеспечение аутентификации;
  - 4) цифровая запись.
  
- 2. Входные параметры процесса шифрования (несколько верных ответов):**
  - 1) зашифрованный текст;
  - 2) ключ;
  - 3) открытый текст;
  - 4) алгоритм.
  
- 3. Какие из сервисов реализуются при использовании криптографических преобразований (несколько верных ответов)?**
  - 1) контроль целостности;
  - 2) аутентификация;
  - 3) масштабирование;
  - 4) архивация.
  
- 4. Какие режимы алгоритма DES пригодны для аутентификации данных?**
  - 1) режимы CBC и CFB пригодны для аутентификации данных;
  - 2) режим ECB обеспечивает аутентификацию данных;
  - 3) ни один из режимов DES не пригоден для аутентификации данных;
  - 4) все режимы DES пригодны для аутентификации данных.
  
- 5. Знание ключа позволяет:**
  - 1) использовать криптографические сервисы безопасности;
  - 2) обеспечить аутентификацию;
  - 3) предотвратить утечку информации;
  - 4) выполнить обратное преобразование.
  
- 6. Что в криптографии понимается под термином “элементарное опробование”?**
  - 1) операция над двумя n-разрядными двоичными числами;
  - 2) проверка ключа на целостность;
  - 3) сопоставление двух паролей;
  - 4) передача ключа по какому-либо каналу связи.



**7. Чем определяется уровень надежности применяемых криптографических преобразований?**

- 1) значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;
- 2) сложностью комбинации символов, выбранных случайным образом;
- 3) использованием большого числа ключей для шифрования;
- 4) отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.

**8. Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее?**

- 1) идентификация и аутентификация пользователей и субъектов доступа;
- 2) управление доступом;
- 3) обеспечение постоянного числа пользователей сети;
- 4) обеспечения целостности;
- 5) регистрация и учет.

**9. Что называется имитовставкой?**

- 1) это блок данных, переменной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты;
- 2) это блок данных фиксированной длины, который вырабатывают по определенному правилу из открытых данных с использованием ключа и затем добавляют к зашифрованным данным для обеспечения их имитозащиты.

**10. Как иначе называется симметричное шифрование?**

- 1) шифрование с закрытым ключом;
- 2) шифрование методом Бейтса;
- 3) шифрование с открытым ключом;
- 4) шифрование с переменным ключом.

**11. Какой алгоритм не используется при симметричном шифровании?**

- 1) алгоритм потокового шифрования;
- 2) алгоритм Rijndael;
- 3) алгоритм блочного шифрования;
- 4) алгоритм Эль-Гамала.

**12. Какой из режимов алгоритма DES используется для построения шифров гаммирования?**

- 1) электронная кодовая книга;
- 2) сцепление блоков шифра;

- 3) обратная связь по шифртексту;
- 4) обратная связь по выходу.

**13. Какова длина блока в алгоритме шифрования DES?**

- 1) 16 бит;
- 2) 56 бит;
- 3) 64 бита;
- 4) 5 байт.

**14. Сколько всего циклов выполняется операция зашифровывания в алгоритме DES?**

- 1) 10;
- 2) 14;
- 3) 16;
- 4) 20.

**15. Что является преимуществом симметричного шифрования?**

- 1) скорость выполнения криптографических преобразований;
- 2) легкость внесения изменений в алгоритм шифрования;
- 3) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
- 5) применение в системах электронной подписи.

**16. Какой размер ключа в отечественном стандарте симметричного шифрования?**

- 1) 56 бит;
- 2) 124 бит;
- 3) 256 бит.

**17. Какой из перечисленных режимов шифрования данных не используется в отечественном стандарте симметричного шифрования?**

- 1) шифрование данных в режиме простой замены;
- 2) шифрование данных в режиме гаммирования;
- 3) шифрование данных в режиме гаммирования с обратной связью;
- 4) выработка имитовставки;
- 5) режим обратной связи по шифртексту;

**18. Использует ли отечественный стандарт симметричного шифрования дополнительную ключевую информацию?**

- 1) да;
- 2) нет.

### 19. Какое из этих утверждений является верным?

- 1) у S-блоков алгоритма DES 6-битовые входы и 4-битовые выходы;
- 2) у S-блоков алгоритма DES 4-битовые входы и 8-битовые выходы;
- 3) у S-блоков алгоритма DES 8-битовые входы и 4-битовые выходы.

### 20. Что означает «многократное шифрование» применительно к блочным шифрам?

- 1) повторное применение алгоритма шифрования к шифртексту с теми же ключами;
- 2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
- 3) повторное применение алгоритма шифрования к шифртексту с другими ключами;
- 4) увеличение числа этапов шифрования открытого текста.

## Примеры практико-ориентированных (ситуационных) заданий

### Примеры контрольных заданий

#### Тема 1. Общие понятия криптографической защиты информации

##### Задача 1

Зашифровать текст при помощи шифра простой замены, при имеющемся ключе. Пропуски не шифруются.

**Текст:** «КРИПТОГРАФИЯ - ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ».

Ключ:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

##### Задача 2

Расшифровать текст при помощи шифра простой замены, при имеющемся ключе шифрования.

**Текст:** «ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

**Ключ-подстановка:**

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Ж	З	Х	К	И	Ц	Ч	Л	А	В	Ъ	Ы	Ь	Б	Д	Г	Е	Ю	Э	Я	П	Р	У	С	Ф	Ш	Т	Щ	М	Н	О

##### Задача 3

Зашифровать текст при помощи шифра перестановки при имеющемся ключе.

**Текст:** «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

#### Задача 4

Расшифровать текст, зашифрованный шифром перестановки, имея ключ

Текст: «ПОРИКТФЧРАГИА СКЕЯИААЩЗТ»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

#### Задача 5

Зашифровать текст с помощью шифра случайного гаммирования, считая, что буквы алфавита пронумерованы от 0 до 32 соответственно. Зная определенную гамму.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Текст: «КРИПТОГРАФИЯ»

Гамма(ключ):

11	1	17	1	14	19	9	14	19	17	15	11
----	---	----	---	----	----	---	----	----	----	----	----

#### Задача 6

Расшифровать криптограмму, полученную с помощью метода случайного гаммирования, считая, что буквы алфавита пронумерованы от 0 до 32 соответственно. Зная определенную гамму.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

**Текст:** «ХСЦРАБЛЮТЕЧЙ»

Гамма(ключ):

11	1	17	1	14	19	9	14	19	17	15	11
----	---	----	---	----	----	---	----	----	----	----	----

### Задача 7

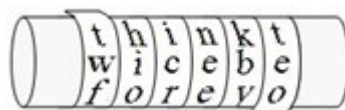
Про составленный из цифр 9-значный пароль  $(a_1, a_2, \dots, a_9)$  известно следующее:

- 1) сумма первых 5-ти цифр  $(a_1 + \dots + a_5)$  делится на 5 без остатка;
- 2) сумма всех 9-ти цифр пароля  $(a_1 + \dots + a_9)$  делится на 10 без остатка.

Сколько существует таких паролей?

### Задача 8

Для шифрования сообщений абоненты  $A$  и  $B$  использовали шифр «Считала»: на круглый стержень виток к витку без просветов и нахлёстов наматывалась лента.



При горизонтальном положении стержня на ленту по всей длине стержня построчно записывался текст сообщения без знаков препинания и пробелов. После этого лента с записанным на ней текстом посылалась адресату. Абонент  $A$  передал абоненту  $B$  ленту, на которой было написано следующее:

з	е	г	л	а	з	а	г	н	а	д	о	л	д	о	з	н	в	л	о	ю	н	о	р	н	в	н	у	я	у	д	о	у	д	е	л	е	б	т	т	к	е	а	г	л	д	е	
е	о	о	н	у	а	г	а	р	о	г	р	л	о	м	т	т	о	я	о	я	ь	н	о	о	ь	о	н	л	т	я	л	е	б	т	а												

К сожалению, абонент  $B$  свой стержень потерял, но  $B$  видит, что лента исписана полностью, и знает, что при намотке ленты было сделано целое число оборотов.

Помогите абоненту  $B$  восстановить сообщение.

### Теоретические вопросы для подготовки к зачету

1. Краткие сведения из истории криптографии.
2. Классификация классических криптоалгоритмов, примеры реализации моноалфавитных, многоалфавитных подстановок и шифров перестановок.
3. Требования к системам шифрования и примеры их реализации в классических криптографических алгоритмах.
4. Краткий обзор современных симметричных систем шифрования.
5. Краткий обзор современных асимметричных систем шифрования.
6. Базовые определения криптографии (стойкость шифра; объем ключа; помехоустойчивость шифра; имитостойкость шифра; разрастание числа ошибок).
7. Классификация методов криптопреобразований и примеры их реализации.
8. Методы замены. Примеры реализации моноалфавитной и многоалфавитной замены.
9. Шифры гомофонической и полиграммной замены.
10. Перестановочные шифры.
11. Шифры гаммирования.
12. Структурная схема симметричной криптосистемы.
13. Сеть Фейстеля.
14. Обзор современных симметричных алгоритмов блочного шифрования.
15. DES (Data Encryption Standard). Обобщенная схема шифрования.
16. Оценка криптостойкости алгоритма DES (Data Encryption Standard).
17. Режимы работы DES (Data Encryption Standard). ECB Электронная кодовая книга.
18. Режимы работы DES (Data Encryption Standard). CBC Сцепление блоков шифра.
19. Режимы работы DES (Data Encryption Standard). CFB Обратная связь по шифру.
20. Режимы работы DES (Data Encryption Standard). OFB Обратная связь по выходу.
21. Области применения DES (Data Encryption Standard).
22. Симметричные криптографические системы. Алгоритм Blowfish.
23. Сравнение алгоритмов Blowfish и DES.
24. Отечественный стандарт симметричного шифрования. Логика построения шифра.
25. Симметричные криптографические системы. AES Rijndael.
26. Модулярная арифметика. Основные понятия и определения.
27. Алгоритм Евклида для нахождения наибольшего общего делителя.
28. Расширенный алгоритм Евклида.
29. Функция Эйлера.
30. Основы вычислений в конечных полях.
31. Обобщенная схема асимметричной системы шифрования. Общие понятия и определения.
32. Алгоритм открытого распределения ключей Диффи–Хеллмана (Diffie -

Hellman).

33. Алгоритм RSA (Rivest-Shamir-Adleman).

34. Алгоритм Эль-Гамала (El Gamal).

35. Электронная подпись (ЭП). Общие понятия и определения, требования и структура ЭП.

36. Процедуры постановки и проверки подлинности ЭП.

37. Схема формирования ЭП (на примере использования алгоритма RSA).

38. Основные требования к цифровым подписям, квалифицированная и неквалифицированная ЭП, согласно №63-ФЗ «Об электронной подписи».

39. ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», основные положения.

40. Перспективы использования электронной подписи в организации электронного документооборота (правовые и экономические аспекты).

41. Хэш-функции: определение и общие требования.

42. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.

43. Методы управления криптографическими ключами.

44. Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17.

45. Хранение криптографических ключей. Иерархия криптографических ключей.

46. Схема аутентификации мастер-ключа.

47. Схема защиты сеансового ключа.

48. Распределение криптографических ключей.

49. Протокол аутентификации и распределения ключей для симметричных криптосистем.

50. Современные приложения криптографии.

51. Перспективы использования методов стеганографии для защиты цифрового контента – плюсы и минусы.

## **8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### **Рекомендуемая литература:**

#### **а) основная литература:**

1. Бабаш А.В., Баранова Е.К., Криптографические методы защиты информации : Учебник / Е.К. Баранова, А.В. Бабаш. – М. : КНОРУС, 2016. – 192 с. URL: <https://avidreaders.ru/book/kriptograficheskie-metody-zaschity-informacii.html> Текст: электронный (дата обращения: 30.09.2022)

2. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. – Лабораторный практикум. – М. КНОРУС, 2015. – 200 с. URL: <https://publications.hse.ru/mirror/pubs/share/direct/478613291.pdf>

Текст: электронный (дата обращения: 30.09.2022)

**б) дополнительная литература:**

3. Фомичев, В.М. Криптографические методы защиты информации.

Ч. 1. Математические аспекты: учебник для академического бакалавриата / В.М. Фомичев, Д.А. Мельников; под ред. В.М. Фомичева. – М.: Издательство Юрайт, 2019. – 209 с. – (Серия: Бакалавр. Академический курс).

URL: <https://urait.ru/bcode/469567>

Текст: электронный (дата обращения: 13.09.2022)

4. Фомичев, В.М. Криптографические методы защиты информации.

Ч. 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичев, Д.А. Мельников; под ред. В.М. Фомичева – М.: Юрайт, 2020. – 246 с. URL: <https://urait.ru/bcode/470279>

Текст: электронный (дата обращения: 13.09.2022)

**9. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины**

1. Справочная правовая система «КонсультантПлюс». [Электронный ресурс].

Режим доступа: <http://www.consultant.ru/>

2. Справочная правовая система «Гарант». [Электронный ресурс]. Режим

доступа: <http://www.garant.ru/iv/>

3. Электронная библиотека Финансового университета (ЭБ)\_<http://elib/fa.ru/>  
(<http://library.fa.ru/elibfa.pdf>)

4. Электронно-библиотечная система BOOK.RU <http://www.book.ru>

5. Электронно-библиотечная система Znanium <http://www.znaniy.com>

6. Научная электронная библиотека eLibrary.ru <http://elibrary.ru>

**10. Методические указания для обучающихся по освоению дисциплины**

Студентам при подготовке следует использовать нормативные документы Финансового университета, а именно – Приказ Финуниверситета от 11.05.2021 №1040/о Об утверждении рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете (см. сайт Финансового Университета: на главной странице раздел «Наш университет»; далее «Единая правовая база Финуниверситета»; подраздел «Организация учебного процесса» – «Нормативные документы по самостоятельной работе»), использовать методические рекомендации кафедр/департаментов.



**11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем**

**11.1. Комплект лицензионного программного обеспечения:**

1. Windows, Microsoft Office
2. Антивирус Kaspersky

**11.2. Современные профессиональные базы данных и информационные справочные системы:**

1. Информационно-правовая система «Гарант».
2. Информационно-правовая система «Консультант Плюс».
3. Электронная энциклопедия: [http://ru.wikipedia.org/wiki/Wiki\\_](http://ru.wikipedia.org/wiki/Wiki_)
4. Система комплексного раскрытия информации «СКРИН»: <http://www.skrin.ru>

**11.3. Сертифицированные программные и аппаратные средства защиты информации:**

Не предусмотрены.

**12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.