

МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Астраханский государственный университет имени В. Н. Татищева»  
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО  
Руководитель ОПОП

О. Н. Выборнова

«05» мая 2025 г.

УТВЕРЖДАЮ

И.о. заведующего кафедрой  
информационной безопасности

В. А. Черкасова

«05» мая 2025 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Составитель(и)

Демина Р.Ю., к.т.н., доц., доцент;  
Выборнова О.Н., к.т.н., доц., доцент;

Согласовано с работодателями:

Давидюк Н.В., доцент, к.т.н., заведующий кафедрой  
«Информационная безопасность», Астраханский  
государственный технический университет;  
Барсуков В.А., начальник отдела информационной  
безопасности Управления корпоративной защиты  
ООО «Газпром добыча Астрахань»;

Направление подготовки /  
специальность

**10.03.01 Информационная безопасность**

Направленность (профиль) /  
специализация ОПОП

**«Организация и технология защиты  
информации»**

Квалификация (степень)

**бакалавр**

Форма обучения

**Очная, очно-заочная**

Год приёма

**2024**

Курс

**3 (по очной форме)  
3 (по очно-заочной форме) /**

Семестр(ы)

**6 (по очной форме) /  
6 (по очно-заочной форме) /**

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**1.1. Целями освоения дисциплины (модуля) «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»** являются изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

**1.2. Задачи освоения дисциплины (модуля)** - дать основы:

- системного подхода к организации защиты информации, передаваемой, обрабатываемой и хранимой техническими средствами на основе применения криптографических методов;
- принципов проектирования и анализа шифров;
- математических методов, которые используются при проектировании и анализе шифров.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

**2.1. Учебная дисциплина (модуль) «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»** относится к обязательной части и осваивается в 6 семестре.

**2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):**

- «Математические основы защиты информации»;
- «Вероятностно-статистические методы в анализе данных»;
- «Теория информации»

**Знания:** основных понятий математики, теории вероятностей и математической статистики, основные теории информации и кодирования, методы эффективного и помехоустойчивого кодирования информации

**Умения:** кодировать цифровые данные, решать типовые задачи теории вероятностей и математической статистики.

**Навыки:** владеть методами количественного анализа процессов обработки, поиска и передачи информации, методикой эффективного кодирования по Хаффману.

**2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):**

1. Основы управления информационной безопасностью.
2. Проектирование и эксплуатация защищенных информационных систем.
3. Криптографические протоколы.

Также дисциплина «Методы и средства криптографической защиты информации» поможет студентам при реализации задач преддипломной практики и написанию бакалаврской работы.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующей(их) компетенции(ий) в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки / специальности: ОПК-9 - способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

**Таблица 1. Декомпозиция результатов обучения**

Код компетенции	Код и наименование индикатора достижения компетенции <sup>1</sup>	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ОПК-9	ОПК-9.1	принципы работы средств криптографической и технической защиты информации для решения стандартных задач профессиональной деятельности.	применять программные программно-аппаратные криптографические и технические средства защиты информации для решения задач профессиональной деятельности.	навыками применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 5 зачетных единиц (180 часов).

Трудоемкость отдельных видов учебной работы студентов очной, очно-заочной форм обучения приведена в таблице 2.1.

**Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения**

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
Объем дисциплины в зачетных единицах	5	5
Объем дисциплины в академических часах	180	180
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	86	46
- занятия лекционного типа, в том числе:	34	15
- практическая подготовка (если предусмотрена)		
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	51	30
- практическая подготовка (если предусмотрена)		
- консультация (предэкзаменационная)	1	1
Самостоятельная работа обучающихся (час.)	94	134
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	экзамен – 6 семестр	экзамен – 6 семестр

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

**Таблица 2.2. Структура и содержание дисциплины (модуля)**

*для очной формы обучения*

Раздел, тема дисциплины (модуля)	Контактная работа, час.						КР / КП	СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточ ной аттестации
	Л		ПЗ		ЛР					
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
<b>Семестр 1.</b>										
Введение. Криптография как механизм защиты	2				2			9	13	Входное тестирование. Опрос на экзамене
Традиционные симметричные шифры	4				6			10	20	Отчет лабораторных работ. Опрос на экзамене
Современные симметричные шифры	6				10			9	25	Отчет лабораторной работы. Опрос на экзамене
Алгоритмы распределения ключей	4				6			10	20	Отчет лабораторной работы. Контрольная работа 1. Опрос на экзамене
Асимметричные криптосистемы	4				6			9	19	Отчет лабораторной работы. Опрос на экзамене.
Однонаправленные ХЭШ-функции	2				2			10	14	Отчет лабораторной работы. Опрос на экзамене
Коды аутентификации сообщений-(MAC)	2				4			9	15	Отчет лабораторной работы. Опрос на экзамене
ЭЦП (электронно-цифровая подпись)	2				3			10	15	Контрольная работа 2. Опрос на экзамене
Создание случайных чисел	4				6			9	19	Отчет лабораторной работы. Опрос на экзамене
Протоколы аутентификации	4				6			9	20	Итоговое тестирование. Опрос на экзамене
<b>Консультации</b>									<b>1</b>	
<b>Контроль промежуточной аттестации</b>										<b>Экзамен</b>

<b>ИТОГО за семестр:</b>	<b>34</b>				<b>51</b>			<b>94</b>	<b>180</b>	
<b>Итого за весь период</b>	<b>34</b>				<b>51</b>			<b>94</b>	<b>180</b>	

*для очно-заочной формы обучения*

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости, форма промежуточной аттестации
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП	КР / КП			
Введение. Криптография как механизм защиты	1	0	0	0	2	0	0	13	16	Входное тестирование. Опрос на экзамене
Традиционные симметричные шифры	2	0	0	0	4	0	0	14	20	Отчет лабораторных работ. Опрос на экзамене
Современные симметричные шифры	3	0	0	0	6	0	0	13	22	Отчет лабораторной работы. Опрос на экзамене
Алгоритмы распределения ключей	2	0	0	0	4	0	0	14	20	Отчет лабораторной работы. Контрольная работа 1. Опрос на экзамене
Асимметричные криптосистемы	2	0	0	0	4	0	0	13	19	Отчет лабораторной работы. Опрос на экзамене.
Однонаправленные ХЭШ-функции	1	0	0	0	2	0	0	14	17	Отчет лабораторной работы. Опрос на экзамене
Коды аутентификации сообщений-(MAC)	1	0	0	0	2	0	0	13	16	Отчет лабораторной работы. Опрос на экзамене
ЭЦП (электронно-цифровая подпись)	1	0	0	0	2	0	0	14	17	Контрольная работа 2. Опрос на экзамене
Создание случайных чисел	1	0	0	0	2	0	0	13	16	Отчет лабораторной работы. Опрос на экзамене
Протоколы аутентификации	1	0	0	0	2	0	0	13	16	Итоговое тестирование. Опрос на экзамене

<b>Консультации</b>										<b>I</b>
<b>Контроль промежуточной аттестации</b>										<b>Экзамен</b>
<b>ИТОГО за семестр:</b>	<i>15</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>30</i>	<i>0</i>	<i>0</i>	<i>134</i>	<i>180</i>	
<b>Итого за весь период</b>	<i>15</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>30</i>	<i>0</i>	<i>0</i>	<i>134</i>	<i>180</i>	

*Примечание:* Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; СР – самостоятельная работа

**Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций**

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции	Общее количество компетенций
		ОПК-9	
Введение. Криптография как механизм защиты	16	+	1
Традиционные симметричные шифры	20	+	1
Современные симметричные шифры	22	+	1
Алгоритмы распределения ключей	20	+	1
Асимметричные криптосистемы	19	+	1
Однонаправленные ХЭШ-функции	17	+	1
Коды аутентификации сообщений- (MAC)	16	+	1
ЭЦП (электронно-цифровая подпись)	17	+	1
Создание случайных чисел	16	+	1
Протоколы аутентификации	17	+	1
<b>Итого</b>	<b>180</b>		

### **Краткое содержание каждой темы дисциплины (модуля)**

#### **Введение. Криптография как механизм защиты**

Чем занимается криптография. История науки. Шифрование как метод защиты данных. Алгоритмы шифрования. Современное состояние криптологии.

#### **Традиционные симметричные шифры**

Функциональная схема симметричной криптосистемы. Блочные шифры. Поточные шифры. Алгоритмы симметричного шифрования. Шифры замены. Шифры перестановки. Шифры гаммирования. Шифрование методом замены.

#### **Современные симметричные шифры**

Требования. Общая схема. Виды современных симметричных шифров. Параметры алгоритмов. Алгоритмы DES, AES, ГОСТ 28147-89, ГОСТ 34.10-2018.

#### **Алгоритмы распределения ключей**

Распределение ключевой информации с использованием одного либо нескольких центров распределения ключей. Прямой обмен сеансовыми ключами между пользователями. Протокол Диффи-Хеллмана. Протоколы безопасной удаленной аутентификации пользователей.

### Асимметричные криптосистемы

Обобщенная схема асимметричной криптосистемы шифрования с открытым ключом. Преимущества асимметричных криптографических систем перед симметричными криптосистемами. Недостатки асимметричных криптосистем.

### Однонаправленные ХЭШ-функции

Построение однонаправленной хэш-функции. Основы построения хэш-функций. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Алгоритм MD5. Алгоритм безопасного хэширования SHA. Отечественный стандарт хэш-функции. Российский стандарт ГОСТ Р 34.11-94

### Коды аутентификации сообщений-(MAC)

Понимание кода аутентификации сообщения (MAC). Алгоритмы, используемые для генерации MAC-адресов. Коды целостности сообщений (MIC).

### ЭЦП (электронно-цифровая подпись)

Алгоритм цифровой подписи RSA. Обобщенная схема цифровой подписи RSA. Недостатки алгоритма цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамала (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. ГОСТ Р 34.10-94.

### Создание случайных чисел

Алгоритмы случайных чисел. Метод Фибоначчи с запаздываниями. Недостатки генераторов псевдослучайных чисел. Инициализация генератора псевдослучайной последовательности.

### Протоколы аутентификации

Аутентификация по паролю. HTTP authentication. Forms authentication. Распространенные уязвимости и ошибки реализации. Аутентификация по сертификатам. Аутентификация по одноразовым паролям. Аутентификация по ключам доступа. Аутентификация по токенам. Форматы токенов. Стандарт SAML. Стандарты WS-Trust и WS-Federation. Стандарты OAuth и OpenID Connect

## 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

Для проведения практических занятий необходима аудитория с проектором и доской. Для проведения лабораторных занятий требуется компьютерный класс с установленными средами разработки на языках программирования высокого уровня.

### 5.2. Указания для обучающихся по освоению дисциплины (модулю)

#### Таблица 4. Содержание самостоятельной работы обучающихся

##### для очной формы обучения

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Периоды развития криптографии (до Шеннона, от Шеннона до Диффи и Хеллмана).	9	Входное тестирование.
История развития криптографии (считаль Лесандра, шифр Цезаря, шифр перестановки, квадрат Полибия, двойной квадрат, шифр Плейфера, многоалфавитные шифры замены, одноразовый блокнот и др.)	10	Отчет лабораторной работы.

Периоды развития криптографии (до Шеннона, от Шеннона до Диффи и Хеллмана).	9	Входное тестирование.
Организационные меры, сопровождающие применение современных симметричных шифров на предприятиях.	9	Отчет лабораторной работы.
Предварительное распределение ключей	10	Отчет лабораторной работы. Контрольная работа 1
Эллиптические кривые	9	Отчет лабораторной работы.
Атаки на хэш-функции	10	Отчет лабораторной работы.
Характеристики оптимальных кодов аутентификации	9	Отчет лабораторной работы.
Схема цифровой подписи вслепую	10	Контрольная работа 2.
Аппаратная генерация случайных чисел	9	Отчет лабораторной работы.
Доказательство полноты и корректности протоколов Фиата-Шамира и Шнорра	9	Итоговое тестирование.

**для очно-заочной формы обучения**

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
Периоды развития криптографии (до Шеннона, от Шеннона до Диффи и Хеллмана).	13	Входное тестирование.
История развития криптографии (считать Лесандра, шифр Цезаря, шифр перестановки, квадрат Полибия, двойной квадрат, шифр Плейфера, многоалфавитные шифры замены, одноразовый блокнот и др.)	14	Отчет лабораторной работы.
Организационные меры, сопровождающие применение современных симметричных шифров на предприятиях.	13	Отчет лабораторной работы.
Предварительное распределение ключей	14	Отчет лабораторной работы. Контрольная работа 1
Эллиптические кривые	13	Отчет лабораторной работы.
Атаки на хэш-функции	14	Отчет лабораторной работы.
Характеристики оптимальных кодов аутентификации	13	Отчет лабораторной работы.
Схема цифровой подписи вслепую	14	Контрольная работа 2.
Аппаратная генерация случайных чисел	13	Отчет лабораторной работы.
Доказательство полноты и корректности протоколов Фиата-Шамира и Шнорра	14	Итоговое тестирование.

**5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно**

*Лабораторные работы.* Для подготовки необходимо изучить теоретический материал по соответствующей теме и разработать программное обеспечение на любом языке программирования. Отчет должен быть представлен в печатном виде и включать в себя описание алгоритма, скриншоты разработанных интерфейсов. При сдаче необходимо продемонстрировать корректно работающее программное обеспечение.

*Контрольные работы.* Для подготовки к контрольной работе необходимо изучить теоретический

материал по соответствующей теме. При написании контрольной работы необходимо развернуто ответить на вопросы, дать аргументированный ответ, привести примеры, подтверждающие точку зрения.

*Тестирование.* Для подготовки к тестированию необходимо изучить теоретический материал по соответствующей теме. При написании теста необходимо выбрать правильный вариант ответа из предложенных.

## 6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

### 6.1. Образовательные технологии

**Таблица 5. Образовательные технологии, используемые при реализации учебных занятий**

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Введение. Криптография как механизм защиты	Обзорная лекция	Не предусмотрено	выполнение теста
Традиционные симметричные шифры	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Современные симметричные шифры	Лекция	Не предусмотрено	выполнение лабораторной, контрольной работы
Алгоритмы распределения ключей	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Асимметричные криптосистемы	Лекция	Не предусмотрено	выполнение лабораторной работы
Однонаправленные ХЭШ-функции	Лекция-диалог	Не предусмотрено	выполнение лабораторной работы
Коды аутентификации сообщений-(MAC)	Лекция	Не предусмотрено	выполнение лабораторной работы
ЭЦП (электронно-цифровая подпись)	Обзорная лекция	Не предусмотрено	выполнение контрольной работы
Создание случайных чисел	Лекция	Не предусмотрено	выполнение лабораторной работы
Протоколы аутентификации	Лекция-диалог	Не предусмотрено	выполнение теста

На практических занятиях применяются следующие образовательные технологии: интерактивные лекции, групповые дискуссии, тематические дискуссии, групповая консультация.

На лабораторных занятиях применяются ролевые игры, учащиеся рассматривают применение криптографических алгоритмов, атаки на них и меры защиты, примеряя на себя роли участников информационного обмена и криптоаналитиков.

Учебные занятия по дисциплине могут проводиться с применением информационно-

телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

## 6.2. Информационные технологии

При организации учебной и внеучебной работы используются возможности сети Интернет, учебные пособия и литература в электронном виде, презентации. Отправка отчетов и рефератов на проверку возможна на электронный адрес (kafedra\_ib\_agu@mail.ru).

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- использование возможностей интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- использование виртуальной обучающей среды (или системы управления обучением LMS Moodle «Электронное образование») или иных информационных систем, сервисов и мессенджеров]

## 6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

### 6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
Microsoft Visual Studio	Среда разработки

### 6.3.2. Современные профессиональные базы данных и информационные справочные системы

- Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: <https://library.asu.edu.ru>.

- Электронный каталог «Научные журналы АГУ»: <http://journal.asu.edu.ru/>.
- Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: <http://dlib.eastview.com/>
- Электронно-библиотечная система elibrary. <http://elibrary.ru>
- Справочная правовая система КонсультантПлюс: <http://www.consultant.ru>
- Информационно-правовое обеспечение «Система ГАРАНТ»: <http://garant-astrakhan.ru>

## **7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

### **7.1. Паспорт фонда оценочных средств**

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Методы и средства криптографической защиты информации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

**Таблица 6. Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств**

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.	Введение. Криптография как механизм защиты	ОПК-9	Входное тестирование. Опрос на экзамене
2.	Традиционные симметричные шифры	ОПК-9	Отчет лабораторных работ. Опрос на экзамене
3.	Современные симметричные шифры	ОПК-9	Отчет лабораторной работы. Опрос на экзамене
4.	Алгоритмы распределения ключей	ОПК-9	Отчет лабораторно й работы. Контрольная работа 1. Опрос на экзамене
5.	Асимметричные криптосистемы	ОПК-9	Отчет лабораторно й работы. Опрос на экзамене.
6.	Однонаправленные ХЭШ- функции	ОПК-9	Отчет лабораторно й работы. Опрос на экзамене
7.	Коды аутентификации сообщений-(MAC)	ОПК-9	Отчет лабораторно й работы. Опрос на экзамене
8.	ЭЦП (электронно-цифровая подпись)	ОПК-9	Контрольная работа 2. Опрос на экзамене
9.	Создание случайных чисел	ОПК-9	Отчет лабораторно й работы. Опрос на экзамене
10.	Протоколы аутентификации	ОПК-9	Итоговое тестирование. Опрос на экзамене

## 7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

**Таблица 7. Показатели оценивания результатов обучения в виде знаний**

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

**Таблица 8. Показатели оценивания результатов обучения в виде умений и владений**

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

## 7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

### Тема «Введение. Криптография как механизм защиты»

#### 1. Входное тестирование

Примерные тестовые вопросы

ТВ	НВ	Вопрос/Ответ
1	1	Несанкционированное копирование программ и данных является:
		Нарушением работоспособности компьютерной сети.
		Преднамеренной угрозой конфиденциальности информации.
		Угрозой нарушения целостности информации.
		Нарушением целостности компонента или ресурса системы.
1	2	«Маскарад» представляет собой:

ТВ	НВ	Вопрос/Ответ
		Способ и прием несанкционированного доступа. Угрозу целостности и работоспособности системы. Разрушение информации, вызванное вирусными воздействиями. Кражу магнитных носителей, содержащих конфиденциальную информацию.
1	3	«Троянский конь» - это: Программа расшифровки шифротекста. Программа хищения информации и разрушения программного обеспечения. Программа стеганографического закрытия информации. Программа шифрования информации методом гаммирования.
1	4	Создание замкнутой среды исполнения программ обеспечивает: Защиту от вредоносных программ (вирусов, «червей» и т. д.). Предотвращает нападение на аппаратные средства. Облегчает процесс администрирования. Предотвращает помехи в линии связи.
1	5	Правила обработки информации являются: Морально-этической мерой безопасности. Аппаратно-программным средством защиты. Правовой защитой информации. Административной мерой защиты информации.
1	6	Разграничение доступа к ресурсам АСДВ относится к: Физическим мерам защиты информации. Аппаратно-программным средствам защиты. Правовым мерам защиты. Морально-этическим мерам защиты.
1	7	Контроль целостности данных осуществляется с помощью: Криптографических методов защиты. Правовых методов. Административных методов защиты. Физических методов защиты.
1	8	Одноключевая криптосистема является: Ассиметричной криптосистемой с открытым ключом. Криптосистемой с закрытым ключом. Симметричной криптосистемой.
1	9	Фундаментальное правило криптоанализа заключается в том, что: Стойкость шифра определяется только секретностью ключа. Отсутствует алгоритм шифрования. Криптоаналитик не имеет в своем распоряжении открытый и шифротекст.
	10	Системы идентификации и аутентификации пользователей относятся к Физическим методам защиты компьютерных сетей Аппаратно-Программным средствам защиты информации Административным методам защиты Правовым методам защиты

### Тема «Традиционные симметричные шифры»

#### 1. Лабораторная работа «Программная реализация любого традиционного шифра перестановки»

Задание:

Разработать программу, реализующую один из традиционных симметричных шифров перестановки: реализовать процедуры шифрования и расшифрования.

Контрольные вопросы:

- Понятие шифрования, ключа шифрования, криптостойкости.
  - Перестановка, замена, гаммирование, метод аналитических преобразований.
- 2. Лабораторная работа** «Программная реализация любого традиционного шифра одноалфавитной замены»

Задание:

Разработать программу, реализующую один из традиционных симметричных шифров перестановки: реализовать процедуры зашифрования и расшифрования.

Контрольные вопросы:

- Понятие шифрования, ключа шифрования, криптостойкости.
- Перестановка, замена, гаммирование, метод аналитических преобразований.

- 3. Лабораторная работа** «Программная реализация любого традиционного шифра полиалфавитной замены»

Задание:

Разработать программу, реализующую один из традиционных симметричных шифров перестановки: реализовать процедуры зашифрования и расшифрования.

Контрольные вопросы:

- Понятие шифрования, ключа шифрования, криптостойкости.
- Перестановка, замена, гаммирование, метод аналитических преобразований.

- 4. Лабораторная работа** «Криптоанализ»

Задание:

Написать программу дешифрования шифртекста, зашифрованного традиционным шифром.

Предусмотреть возможность ввода текста как интерактивно с клавиатуры, так и из файла.

Контрольные вопросы:

- Понятие криптоанализа
- В чем заключается шифрование методом Вижинера
- В чем заключается криптоанализ текста, зашифрованного методом Вижинера?

### **Тема «Современные симметричные шифры»**

- 1. Лабораторная работа** «Программная реализация алгоритма шифрования DES»

Задание:

Написать на языке высокого уровня программу, которая бы реализовывала алгоритм шифрования/расшифрования DES

Контрольные вопросы:

1. Сеть Фейстеля
2. Общая схема DES
3. Создание подключей
4. Недостатки двойного DES
5. Тройной DES с двумя ключам

- 2. Лабораторная работа** «Программная реализация алгоритма шифрования ГОСТ Магма»

Задание:

Написать на языке высокого уровня программу, которая бы реализовывала алгоритм шифрования / расшифрования «Магма»

Контрольные вопросы:

1. Общая схема, функция F, генерация ключей.
2. Основные режимы шифрования
3. Основные различия между ГОСТ и DES.

### 3. Лабораторная работа «Программная реализация алгоритма шифрования ГОСТ Кузнечик»

#### Задание:

Написать на языке высокого уровня программу, которая бы реализовывала алгоритм шифрования / расшифрования «Кузнечик»

Контрольные вопросы:

1. Общая схема, функция F, генерация ключей.
2. Основные режимы шифрования
3. SP-сеть

#### Тема «Алгоритмы распределения ключей»

##### 1. Контрольная работа 1

Вопросы к контрольной работе № 1:

1. Криптография – как механизм защиты информации. Безопасность информации и защита информации. Основные нарушения безопасности. Политика безопасности. Уязвимость, атака, риск. Классификация сетевых атак. Виды активных атак. Механизмы и сервисы безопасности.
2. Определения шифра, ключа шифрования. Понятие криптоанализа. Основные типы криптоаналитического вскрытия. Категории вскрытия криптоалгоритмов. Безусловная и вычислительная криптостойкость. Основные требования к шифрам для криптозащиты информации. Основные типы шифров.
3. Шифры перестановки: скитала, табличное шифрование, двойная перестановка, магические квадраты.
4. Шифры простой замены: полибианский квадрат, система Цезаря, аффинная система Цезаря, система Цезаря с ключевым словом, таблицы Трисемуса, биграммный шифр Плейфейра.
5. Криптосистема Хилла.
6. Система омофонов.
7. Шифры сложной замены: шифр Гронсфельда, система Вижинера, двойной квадрат Уинстоне, метод Вернама. Роторные машины.
8. Одноразовая система шифрования.
9. Метод гаммирования.
10. Необходимые и достаточные условия недешифруемости систем шифрования, понятия диффузии и конфузии. Дополнительные требования к алгоритмам шифрования при использовании ЭВТ.
11. Формальные модели шифров. Стойкость шифров. Совершенные шифры. Теорема Шеннона. Практическая стойкость шифра.
12. Сеть Фейстеля: архитектура сети, сеть с несколькими раундами, разбалансированная сеть, гетерогенные и гомогенные сети.
13. Алгоритм DES: принципы разработки, общая схема, начальная перестановка, преобразования отдельного раунда, создание подключей, дешифрование, проблемы DES, недостатки двойного DES (атака «встреча посередине»), тройной DES с двумя ключами, слабые ключи.
14. Алгоритм ГОСТ 34.12–2015: общая схема, функция F, генерация ключей.
15. Основные режимы шифрования ГОСТ 34.12–2015.
16. Выработка имитовставки в ГОСТ 34.12–2015. Основные различия между ГОСТ 34.12–2015 и DES.
17. Алгоритм AES Rijndael: используемые математические понятия, критерии разработки, понятие слоя, понятие состояния, ключ шифрования, число раундов, создание ключей раунда, расширение ключа. Преимущества алгоритма.
18. Преобразования раунда в алгоритме Rijndael (ByteSub, ShiftRow, MixColumn, сложение с ключом раунда), предварительное забеливание с использованием ключа.

19. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB). Распространение ошибок.
20. Объединение блочных шифров. Двойное и тройное шифрование (с 2 ключами, с 3 ключами, с минимальным ключом). Режимы тройного шифрования. Отбеливание. Многократное последовательное использование блочных алгоритмов.
21. Алгоритмы распределения ключей. Понятие мастер-ключа. Алгоритм обмена ключом Диффи-Хеллмана.

## **2. Лабораторная работа «Программная реализация алгоритма шифрования AES»**

Задание:

Написать на языке высокого уровня программу, которая бы реализовывала алгоритм шифрования/расшифрования AES

Контрольные вопросы:

1. Критерии разработки.
2. Понятия состояния.
3. Ключ шифрования.
4. Число раундов.
5. Преимущество алгоритма.

### **Тема «Асимметричные криптосистемы»**

#### **1. Лабораторная работа «Программная реализация любого асимметричного шифра»**

Задание:

Написать на языке высокого уровня программу, которая бы реализовывала асимметричный алгоритм шифрования/расшифрования (например, алгоритм RSA, Эль-Гамала)

Контрольные вопросы:

1. Понятие асимметричного шифрования
2. Достоинства, недостатки
3. Алгоритм RSA
4. Алгоритм Эль-Гамала

### **Темы «Однонаправленные ХЭШ-функции», «Коды аутентификации сообщений-(MAC)»**

#### **1. Лабораторная работа «Программная разработка системы обмена сообщениями с кодами аутентификации сообщений»**

Задание:

Написать на языке высокого уровня программу, которая бы имитировала передачу текстовых сообщений, а также реализовывала проверку их целостности и аутентичности. Для формирования MAC может быть использован любой алгоритм, в т.ч. на основе использования хэш-функций.

Контрольные вопросы:

1. Свойства безопасности: целостность, аутентичность, неотказуемость.
2. Понятие хэш-функции, алгоритмы, коллизии.
3. Понятие MAC, алгоритмы.

### **Тема «ЭЦП (электронно-цифровая подпись)»**

#### **1. Контрольная работа 2**

Вопросы к контрольной работе № 2:

1. Основные требования к алгоритмам асимметричного шифрования. Основные способы использования алгоритмов с открытым ключом. Криптоанализ алгоритмов с открытым ключом.
2. Алгоритм RSA: описание алгоритма, вычислительные аспекты шифрования/расшифрования и создания ключей, криптоанализ алгоритма.

3. Схема шифрования Эль Гамалья.
4. Комбинированный метод шифрования.
5. Хэш-функции: основные требования, простые хэш-функции, парадокс «дней рождения». Использование цепочки зашифрованных блоков, хэш-функция Рабина.
6. Хэш-функция MD5: логика выполнения. Отличия от хэш-функции MD4.
7. Хэш-функция SHA-1: логика выполнения. Сравнение MD5 и SHA-1.
8. Хэш-функция SHA-2: логика выполнения.
9. Хэш-функция ГОСТ 34.11: логика выполнения. Алгоритм обработки одного блока.
10. Требования к MAC.
11. MAC на основе алгоритма симметричного шифрования.
12. MAC на основе хэш-функции, HMAC.
13. ЭЦП: определение, предназначение, состав.
14. Алгоритмы ЭЦП: RSA, EGSA (Эль Гамалья), DSA, ГОСТ.

### Тема «Создание случайных чисел»

#### 1. Лабораторная работа «Исследование свойств любого генератора псевдослучайных чисел»

Задание:

Реализовать любой генератор псевдослучайных чисел. Исследовать свойства генератора.

Контрольные вопросы:

1. Требования к случайным числам (СЧ).
2. Источники СЧ.
3. Генераторы псевдо-СЧ.
4. Криптографически созданные СЧ.

### Тема «Протоколы аутентификации»

#### 1. Итоговое тестирование

Примерные тестовые вопросы:

ТВ	НВ	Вопрос/Ответ
2	1	Шифрование перестановкой заключается
		Перестановке символов шифруемого текста по определённому правилу
		Замене символов шифруемого текста символами того же или другого алфавита
		Сложении символов шифруемого текста с символами некоторой случайной последовательности
		Преобразовании шифруемого текста по некоторому аналитическому правилу
2	2	Шифрование заменой заключается
		Перестановке символов шифруемого текста по определённому правилу
		Замене символов шифруемого текста символами того же или другого алфавита
		Сложении символов шифруемого текста с символами некоторой случайной последовательности
		Преобразовании шифруемого текста по некоторому аналитическому правилу
2	3	Шифрование гаммированием заключается
		Перестановке символов шифруемого текста по определённому правилу
		Замене символов шифруемого текста символами того же или другого алфавита
		Сложении символов шифруемого текста с символами некоторой случайной последовательности
		Преобразовании шифруемого текста по некоторому аналитическому правилу
2	4	Шифрование аналитическим преобразованием заключается в
		Перестановке символов шифруемого текста по определённому правилу
		Замене символов шифруемого текста символами того же или другого алфавита

ТВ	НВ	Вопрос/Ответ
		Сложение символов шифруемого текста с символами некоторой случайной последовательности
		Преобразовании шифруемого текста по некоторому аналитическому правилу
2	5	Размер и особенности структуры таблицы являются
		Средством для размещения шифруемого текста
		Ключом шифра
		Алгоритмом шифрования
2	6	Магические квадраты относятся к
		Шифрам гаммирования
		Шифрам перестановки
		Шифрам замены
		Шифрования аналитическим преобразованием
2	7	Система шифрования Цезаря относится к
		Шифрам простой замены
		Шифрам сложной замены
		Шифрованию гаммирования
		Шифрования перестановкой
2	8	Достоинством системы шифрования Цезаря
		Не маскируется частота появления букв открытого текста
		Простота шифрования и расшифрования
		Сохраняется алфавитный порядок в последовательности заменяющих букв
2	9	Аффинная система подстановок Цезаря является
		Шифрованием методом перестановки
		Шифрованием методом замены
		Шифрованием гаммирования
2	10	Шифрующие таблицы Трисемуса являются
		Шифрованием методом простой замены
		Шифрованием методом перестановки
		Шифрованием методом гаммирования
		Шифрованием методом аналитического преобразования
2	11	Биграммный шифр Плейфейра является
		Шифрованием методом перестановок
		Шифрованием методом замены
		Шифрованием гаммированием
2	12	Криптосистема Хилла является
		Шифрованием методом простой замены
		Шифрованием методом перестановок
		Шифрованием методом гаммированием
		Шифрованием методом аналитического преобразования
2	13	Шифры сложной замены являются
		Одноалфавитными шифрами
		Многоалфавитными шифрами
		Шифрованием гаммированием
2	14	Система шифрованием Вижинера
		Система шифрования простой замены
		Система шифрованием сложной замены
		Система одноалфавитного шифрования
2	15	Шифр “двойной квадрат“ Уитстона
		Шифр простой замены

ТВ	НВ	Вопрос/Ответ
		Одноалфавитный шифр
		Многоалфавитный шифр
2	16	Одноразовая система шифрования
		Абсолютно надежна при случайном наборе ключей
		Позволяет надежно шифровать тексты с многими миллионами символов
		Абсолютно надежна при выборе ключей по определенному алгоритму
2	17	Шифрование методом Вернама является
		Частным случаем системы шифрования Цезаря
		Частным случаем таблиц Трисемуса
		Частным случаем одноразовой системой шифрования
2	18	Для генерирования непредсказуемых двоичных последовательностей ключей используется
		Генераторы двоичных псевдослучайных последовательностей
		Алгоритмы для расчета ключей
		Длинная ключевая последовательность, представленная в компактной форме
3	19	Современные симметричные криптосистемы базируются на принципах
		Рассеивания и перемешивания
		Шифрования методом перестановки
		Шифрования методом гаммирования
3	20	Шифрования данных DES
		Имеет только один ключ длиной 56 бит
		Имеет последовательность ключей
		Имеет несколько ключей длиной 64 бит каждый
3	21	Алгоритм DES осуществляет шифрование
		32-битовых блоков данных с помощью 64-битового ключа
		56-битовых блоков данных с помощью 56-битового ключа
		64-битовых блоков данных с помощью 64-битового ключа, с 56 значащими битами
3	22	Одним из основных режимов работы алгоритма DES является
		Электронная кодовая книга ECB (Electronic Code Book)
		Шифрование данных со скоростью 2,4 Мбит/с
		Шифрование данных со скоростью 4,8 Мбит/с
		Одним из основных режимов работы алгоритма
3	23	Одним из основных режимов работы алгоритма DES является
		Сцепление блоков шифра CBC (Cipher Block Chaining)
		Шифрование с депонированием ключа
		Шифрование данных со скоростью 2,4 Мбит/с

### Перечень вопросов к экзамену

1. Криптография – как механизм защиты информации. Безопасность информации и защита информации. Основные нарушения безопасности. Политика безопасности. Уязвимость, атака, риск. Классификация сетевых атак. Виды активных атак. Механизмы и сервисы безопасности.
2. Определения шифра, ключа шифрования. Понятие криптоанализа. Основные типы криптоаналитического вскрытия. Категории вскрытия криптоалгоритмов. Безусловная и вычислительная криптостойкость. Основные требования к шифрам для криптозащиты информации. Основные типы шифров.
3. Шифры перестановки: скитала, табличное шифрование, двойная перестановка, магические квадраты.

4. Шифры простой замены: полибианский квадрат, система Цезаря, аффинная система Цезаря, система Цезаря с ключевым словом, таблицы Трисемуса, биграммный шифр Плейфейра.
5. Криптосистема Хилла.
6. Система омофонов.
7. Шифры сложной замены: шифр Гронсфельда, система Вижинера, двойной квадрат Уитстона, метод Вернама. Роторные машины.
8. Одноразовая система шифрования.
9. Метод гаммирования.
10. Необходимые и достаточные условия недешифруемости систем шифрования, понятия диффузии и конфузии. Дополнительные требования к алгоритмам шифрования при использовании ЭВТ.
11. Формальные модели шифров. Стойкость шифров. Совершенные шифры. Теорема Шеннона. Практическая стойкость шифра.
12. Сеть Фейстеля: архитектура сети, сеть с несколькими раундами, разбалансированная сеть, гетерогенные и гомогенные сети.
13. Алгоритм DES: принципы разработки, общая схема, начальная перестановка, преобразования отдельного раунда, создание подключей, дешифрование, проблемы DES, недостатки двойного DES (атака «встреча посередине»), тройной DES с двумя ключами, слабые ключи.
14. Алгоритм ГОСТ Магма: общая схема, функция F, генерация ключей.
15. Алгоритм ГОСТ Кузнечик
16. Основные режимы шифрования ГОСТ 34.12— 2015.
17. Выработка имитовставки в ГОСТ 34.12— 2015. Основные различия между ГОСТ 34.12— 2015 и DES.
18. Алгоритм AES Rijndael: используемые математические понятия, критерии разработки, понятие слоя, понятие состояния, ключ шифрования, число раундов, создание ключей раунда, расширение ключа. Преимущества алгоритма.
19. Преобразования раунда в алгоритме Rijndael (ByteSub, ShiftRow, MixColumn, сложение с ключом раунда), предварительное забеливание с использованием ключа.
20. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB). Распространение ошибок.
21. Объединение блочных шифров. Двойное и тройное шифрование (с 2 ключами, с 3 ключами, с минимальным ключом). Режимы тройного шифрования. Отбеливание. Многократное последовательное использование блочных алгоритмов.
22. Алгоритмы распределения ключей. Понятие мастер-ключа. Алгоритм обмена ключом Диффи-Хеллмана.
23. Основные требования к алгоритмам асимметричного шифрования. Основные способы использования алгоритмов с открытым ключом. Криптоанализ алгоритмов с открытым ключом.
24. Алгоритм RSA: описание алгоритма, вычислительные аспекты шифрования/расшифрования и создания ключей, криптоанализ алгоритма.
25. Схема шифрования Эль Гамала.
26. Комбинированный метод шифрования.
27. Хэш-функции: основные требования, простые хэш-функции, парадокс «дней рождения». Использование цепочки зашифрованных блоков, хэш-функция Рабина.
28. Хэш-функция MD5: логика выполнения. Отличия от хэш-функции MD4.
29. Хэш-функция SHA-1: логика выполнения. Сравнение MD5 и SHA-1.
30. Хэш-функция SHA-2: логика выполнения.
31. Хэш-функция ГОСТ 34.11: логика выполнения. Алгоритм обработки одного блока.
32. Требования к MAC.
33. MAC на основе алгоритма симметричного шифрования.

34. MAC на основе хэш-функции, HMAC.  
 35. ЭЦП: определение, предназначение, состав.  
 36. Алгоритмы ЭЦП: RSA, EGSA (Эль Гамала), DSA, ГОСТ Р 34.10.  
 37. Требования к случайным числам (СЧ). Источники СЧ. Генераторы псевдо-СЧ.  
 38. Криптографически созданные СЧ.

**Таблица 9 – Примеры оценочных средств с ключами правильных ответов**

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности				
1.	Задание закрытого типа	Какой шифр не основан на шифре Цезаря? 1. Афинный шифр 2. Биграммный шифр Плейфера 3. Шифра Вижинера 4. Шифр Гронсфельда	2	5
2.		Какой шифр основан на шифре Цезаря 1. Шифр Гронсфельда 2. RSA 3. Магический квадрат 4. Квадрат Полибия	1	5
3.		Какая система шифрования является наиболее стойкой ко взлому? 1. AES 2. ГОСТ Р 34.12-2015 3. ГОСТ 28147-89 4. Одноразовый блокнот	4	5
4.		Может ли в криптосистеме «Магический квадрат» для шифрования использоваться таблица, для которой не выполняются требования по равенству сумм в столбцах/строках? 1. Должно выполняться хотя бы одно условие 2. Должны выполняться оба условия 3. Условие равенства сумм в строках/столбцах может и не выполняться.	3	5
5.		В основу каких алгоритмов шифрования легла сеть Фейстеля? 1. DES 2. ГОСТ 28147-89 3. AES 4. ГОСТ Р 34.12-2015	1, 2	5
6.		Задание открытого типа	Сообщение было записано в таблицу (5 строк 7 столбцов) по столбцам, а считано по строкам.	ТЕРМИНАТОР ПРИБЫВАЕТ

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)																
		<p>Зашифрованное сообщение выглядит следующим образом: ТНПВЕ ГЛЕАР АДОНР ТИЕЪВ ОМОБТ МПЧИР ЫСООЪ</p> <p>Какое сообщение было зашифровано?</p>	СЕДЬМОГО ПОЛНОЧЬ В																	
7.		<p>Шифр табличной перестановки. Ключ – ПЕЛИКАН Сообщение записывалось по столбцам, а считывалось построчно Шифротекст - ГНВЕП ЛТООА ДРНЕВ ТЕБИО РПОТМ БЧМОР СОБЬИ Расшифруйте.</p>	ГНВЕП ЛТООА ДРНЕВ ТЕБИО РПОТМ БЧМОР СОБЬИ	5																
8.		<p>С использованием магического квадрата было зашифровано некое сообщение. Сообщение считывалось построчно</p> <table border="1" data-bbox="453 958 759 1137"> <tr><td>16</td><td>3</td><td>2</td><td>13</td></tr> <tr><td>5</td><td>10</td><td>11</td><td>8</td></tr> <tr><td>9</td><td>6</td><td>7</td><td>12</td></tr> <tr><td>4</td><td>15</td><td>14</td><td>1</td></tr> </table> <p>Шифротекст - ОИРМ ЕОСЮ ВТАЪ ЛГОП Расшифруйте.</p>	16	3	2	13	5	10	11	8	9	6	7	12	4	15	14	1	ПРИЛЕТАЮ ВОСЬМОГО	5
16	3	2	13																	
5	10	11	8																	
9	6	7	12																	
4	15	14	1																	
9.		<p>Сообщение было зашифровано шифром Цезаря. Ключ – 2. Алфавит – русский, 33 буквы Шифротекст – СРНМРДРЁЖШ Расшифруйте</p>	ПОЛКОВОДЕЦ	5																
10.		<p>Зашифруйте сообщение с использованием квадрата Полибия. Таблица – 4 строки, 8 столбцов Ключ – Бандероль Алфавит – русский, без буквы Ё Открытый текст – ВЫЛЕТАЕМПЯТОГО. Шифротекст - ?</p>	ПДКЗЫВЗЧШЛЫЙСЙ	5																

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля).

#### 7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Баллы, полученные в течение семестра, суммируются с баллами, полученными на экзамене. Исходя из получившегося результата выставляется итоговая оценка:

- 0-59 баллов – 2, «неудовлетворительно»
- 60-74 баллов – 3, «удовлетворительно»
- 75-89 баллов – 4, «хорошо»
- 90-100 баллов – 5, «отлично»

**Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю) в каждом семестре**

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
<b>Основной блок</b>				
1.	<i>Выполнение лабораторной работы</i>	9/4	36	По расписанию
2.	<i>Выполнение контрольной работы</i>	2/1	2	
3.	<i>Тест</i>	2/1	2	
<b>Всего</b>			<b>40</b>	-
<b>Блок бонусов</b>				
4.	<i>Посещение занятий без пропусков</i>	1	3	
5.	<i>Своевременное выполнение всех заданий</i>	1	3	
6.	<i>Активность студента на занятии</i>	1	4	
<b>Всего</b>			<b>10</b>	-
<b>Дополнительный блок</b>				
7.	<i>Экзамен</i>		50	
<b>Всего</b>			<b>50</b>	-
<b>ИТОГО</b>			<b>100</b>	-

**Таблица 11 – Система штрафов (для одного занятия)**

Показатель	Балл
<i>Опоздание на занятие</i>	- 1
<i>Нарушение учебной дисциплины</i>	- 1
<i>Неготовность к занятию</i>	- 2
<i>Пропуск занятия без уважительной причины</i>	- 2

**Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)**

Сумма баллов	Оценка по 4-балльной шкале
90–100	5 (отлично)
85–89	4 (хорошо)
75–84	
70–74	
65–69	3 (удовлетворительно)
60–64	
Ниже 60	2 (неудовлетворительно)

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

## **8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

1. Криптографические методы защиты информации: Учебное пособие для вузов / Рябко Б.Я., Фионов А.Н. - 2-е издание, стереотип. - М. : Горячая линия - Телеком, 2012. - URL: <http://www.studentlibrary.ru/book/ISBN9785991202862.html> (ЭБС «Консультант студента»).
2. Криптографические методы защиты информации / Аверченков В.И. - М. : ФЛИНТА, 2017. - URL: <http://www.studentlibrary.ru/book/ISBN9785976529472.html> (ЭБС «Консультант студента»).
3. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2015. - (Программисту). - URL: <http://www.studentlibrary.ru/book/ISBN9785996329526.html> (ЭБС «Консультант студента»).
4. Криптографические методы защиты информации. Шифры: учебное пособие / Котов Ю.А. - Новосибирск : Изд-во НГТУ, 2016. - URL: <http://www.studentlibrary.ru/book/ISBN9785778229594.html> (ЭБС «Консультант студента»).
5. Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н. - 2-е изд. - М. : Горячая линия - Телеком, 2013. - URL: <http://www.studentlibrary.ru/book/ISBN9785991203500.html> (ЭБС «Консультант студента»).
6. Системы блочного шифрования: учеб. пособие по курсу "Криптографические методы защиты информации" / А. Е. Жуков. - М. : Издательство МГТУ им. Н. Э. Баумана, 2013. - URL: <http://www.studentlibrary.ru/book/ISBN9785703837535.html> (ЭБС «Консультант студента»).

### **8.2. Дополнительная литература**

1. Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - URL: <http://www.studentlibrary.ru/book/ISBN5980030026.html> (ЭБС «Консультант студента»).
2. Компьютерная безопасность. Криптографические методы защиты / Петров А.А. - М. : ДМК Пресс, 2008. - URL: <http://www.studentlibrary.ru/book/ISBN5898180648.html> (ЭБС «Консультант студента»).

### **8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)**

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. [www.studentlibrary.ru](http://www.studentlibrary.ru).

## **9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Для проведения лекционных занятий необходима мультимедийная аудитория, оснащенная компьютерной презентационной техникой.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

## **10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).