МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ЧЕБОКСАРСКИЙ ИНСТИТУТ (ФИЛИАЛ) МОСКОВСКОГО ПОЛИТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Кафедра Информационных технологий, электроэнергетики и систем управления

УТВЕРЖДАЮ
Директор филиала
________________ А.В. Агафонов
«29» __мая__ 2020г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

(наименование дисциплины)

Направление подготовки	**09.03.01 «Информатика и вычислительная техника»**
	(код и наименование направления подготовки)
Направленность (профиль) подготовки	**«Программное обеспечение вычислительной техники и автоматизированных систем»**
	(наименование профиля подготовки)
Квалификация выпускника	**Бакалавр**
Форма обучения	**очная, заочная**

Чебоксары, 2020

Рабочая программа дисциплины разработана в соответствии с:

- Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 – Информатика и вычислительная техника, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 929 от 19 сентября 2017 г. зарегистрированный в Минюсте 10 октября 2017 года, рег. номер 48489 (далее – ФГОС ВО).

- учебным планом (очной, заочной форм обучения) по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

Рабочая программ дисциплины включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (п.8 Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины)

Автор Матижев Петр Владимирович, заведующий кафедрой ИТЭСУ.
(указать ФИО, ученую степень, ученое звание или должность)

Программа одобрена на заседании кафедры ИТЭСУ (протокол № 10 от 16.05.2020).

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы (Цели освоения дисциплины)

1.1. Целями освоения дисциплины «Криптографические методы защиты информации» являются:

– получение студентами знаний о теоретических основах криптографии;

– формирование навыков работы с современными программными и техническими средствами ЭВМ, обеспечивающими защиту хранимой, обрабатываемой и передаваемой информации от случайного или преднамеренного ознакомления, изменения и уничтожения;

– изучение способов и средств несанкционированного доступа к информации, способов и средств защиты конфиденциальной информации.

1.2. Области профессиональной деятельности и(или) сферы профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии (в сфере проектирования, разработки, внедрения и эксплуатации средств вычислительной техники и информационных систем, управления их жизненным циклом).

1.3. К основным задачам изучения дисциплины относится подготовка обучающихся к выполнению трудовых функций в соответствии с профессиональными стандартами:

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
06.001 Программист Профессиональный стандарт "Программист", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 г. N 679н (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный N 30635), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. N	D	Разработка требований и проектирование программного обеспечения	6	Анализ требований к программному обеспечению	D/01.6	6
			6	Разработка технических спецификаций на программные компоненты и их взаимодействие	D/02.6	
			6	Проектирование программного обеспечения	D/03.6	

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный N 45230)						

1.4. Компетенции обучающегося, формируемые в результате освоения дисциплины

Наименование категории (группы) компетенций	**Код и наименование компетенций**	**Код и наименование индикатора достижения компетенции**	**Перечень планируемых результатов обучения**
	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1 Разрабатывает модели бизнес-процессов заказчика ПК-1.2 Выявляет и анализирует требования к ИС ПК-1.3 Разрабатывает архитектуру ИС ПК-1.4 Проектирует ИС ПК-1.5 Разрабатывает базы данных ИС ПК-1.6 Владеет технологиями программирования ПК-1.7 Владеет технологиями модульного тестирования ИС (верификации) ПК-1.8 Организует репозиторий хранения данных о создании (модификации) и вводе ИС в эксплуатацию ПК-1.9 Создание пользовательской документации к ИС	**Знать:** - стандартные задачи профессиональной деятельности; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - понятия конфиденциальной информации, персональных данных и государственной тайны. **Уметь:** -применять математические методы, вычислительную технику для решения практических задач; - анализировать и выбирать методы и средства обеспечения информационной безопасности. **Владеть:** - элементами функционального

			анализа; - библиотечно-библиографическими знаниями.
	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.1 Разрабатывает драйверы устройств ПК-3.2 Разрабатывает компиляторы, загрузчики, сборщики ПК-3.3 Разрабатывает системные утилиты ПК-3.4. Создает инструментальные средства программирования	**Знать:** - сущность и значение информации в развитии в развитии современного информационного общества; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности. **Уметь:** - выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности. **Владеть:** - численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; - методами и средства обеспечения информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина (Б1.Д(М).В.14) «Криптографические методы защиты информации» реализуется в рамках элективной дисциплины (модуля) программы бакалавриата.

Дисциплина преподается обучающимся по очной форме обучения – во 5-м семестре, по заочной форме – в 6 семестре.

Дисциплина «Криптографические методы защиты информации» является промежуточным этапом формирования компетенций ПК-1, ПК-3 в процессе освоения ОПОП.

Дисциплина «Криптографические методы защиты информации» основывается на знаниях, умениях и навыках, приобретенных при изучении дисциплин: операционные системы, ЭВМ и периферийные устройства, структуры и алгоритмы обработки данных, и является предшествующей для изучения дисциплин: автоматизированные информационно-управляющие системы, методы оптимизации и автоматизации проектирования, системное программирование.

Формой промежуточной аттестации знаний обучаемых по очной форме обучения является зачет во 5-м семестре, по заочной форме зачет в 6 семестре.

3. Объем дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы (72 академических часа), в том числе

очная форма обучения:

Семестр	5
Лекции	16
лабораторные занятия	16
семинары и практические занятия	-
контроль: контактная работа	0,2
контроль: самостоятельная работа	8,8
расчетно-графические работы, курсовые работы (проекты): контактная работа	-
расчетно-графические работы, курсовые работы (проекты): самостоятельная работа	-
Консультации	-
Контактная работа	32,2
Самостоятельная работа	39,8

Вид промежуточной аттестации (форма контроля): зачёт

заочная форма обучения:

Семестр	6
Лекции	4
лабораторные занятия	4
семинары и практические занятия	-
контроль: контактная работа	0,2
контроль: самостоятельная работа	8,8
расчетно-графические работы, курсовые работы (проекты): контактная работа	-
расчетно-графические работы, курсовые работы (проекты): самостоятельная работа	-

Консультации	-
Контактная работа	8,2
Самостоятельная работа	63,8

Вид промежуточной аттестации (форма контроля): зачёт

4. Содержание дисциплины, структурированное по темам (разделам)

Очная форма обучения

Тема (раздел)	Количество часов				Код индикатора достижений компетенции
	контактная работа			самостоятельная работа	
	Лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	4	4	-	7	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	4	4	-	8	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 3. Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	4	4	-	8	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	4	4	-	8	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Контроль (Зачёт)	0,2			8,8	
ИТОГО	**32,2**			39,8	

Заочная форма обучения

Тема (раздел)	Количество часов				Код индикатора достижений компетенции
	контактная работа			самостоятельная работа	
	лекции	лабораторные занятия	семинары и практические занятия		
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	1	1	-	10	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей.	1	1	-	15	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 3. Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	1	1	-	15	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	1	1	-	15	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Контроль (зачет)	0,2			8,8	
ИТОГО	8,2			63,8	

5. Образовательные технологии, применяемые при освоении дисциплины

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование

следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

Основной формой проведения интерактивных занятий по дисциплине «Криптографические методы защиты информации» является разбор конкретных ситуаций.

6. Практическая подготовка

Практическая подготовка реализуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью. Объем занятий в форме практической подготовки составляет 2 часа (по очной форме обучения), 2 часа (по заочной форме обучения).

Очная форма обучения

Вид занятия	Тема занятия	Количество часов	Форма проведения	Код индикатора достижений компетенции
Практическое задание 1	Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	4	Отчёт	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4

Заочная форма обучения

Вид занятия	Тема занятия	Количество часов	Форма проведения	Код индикатора достижений компетенции
Практическое задание 1	Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	2	Отчёт	ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-1.8, ПК-1.9, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4

7. Учебно-методическое обеспечение самостоятельной работы студентов

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 39,8 часов (очная форма обучения) и 63,8 часов (заочная форма обучения).

Самостоятельная работа реализуется в рамках программы освоения дисциплины в следующих формах:

- работа с конспектом занятия (обработка текста);
- работа над учебным материалом учебника;
- проработка тематики самостоятельной работы;
- поиск информации в сети «Интернет» и литературе;
- подготовка к сдаче зачета.

В рамках учебного курса предусматриваются встречи с представителями правоохранительных органов.

Самостоятельная работа проводится с целью: систематизации и закрепления полученных теоретических знаний и практических умений обучающихся; углубления и расширения теоретических знаний студентов; формирования умений использовать нормативную, правовую, справочную документацию, учебную и специальную литературу; развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности; формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации; формирования профессиональных компетенций; развитию исследовательских умений студентов.

Формы и виды самостоятельной работы студентов: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление хронологической таблицы; составление библиографии (библиографической картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, контрольной работе, зачету); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, задачи, тесты; выполнение творческих заданий).

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов образовательного учреждения: библиотеку с читальным залом, компьютерные классы с возможностью работы в Интернет; аудитории (классы) для консультационной деятельности.

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной

самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации.

Самостоятельная работа может осуществляться индивидуально или группами обучающихся в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

Контроль самостоятельной работы студентов предусматривает: соотнесение содержания контроля с целями обучения; объективность контроля; валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить); дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы: просмотр и проверка выполнения самостоятельной работы преподавателем; организация самопроверки, взаимопроверки выполненного задания в группе; обсуждение результатов выполненной работы на занятии; проведение письменного опроса; проведение устного опроса; организация и проведение индивидуального собеседования; организация и проведение собеседования с группой.

№ п/п	Вид учебно-методического обеспечения
1.	Контрольные задания (варианты).
2.	Тестовые задания.
3.	Вопросы для самоконтроля знаний.
4.	Темы докладов.
5.	Типовые задания для проведения текущего контроля успеваемости обучающихся (Тестовые задания, практические ситуативные задачи, тематика докладов и рефератов)
6.	Задания для подготовки к промежуточной аттестации по дисциплине (Вопросы к зачету)

8. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

8.1. Паспорт фонда оценочных средств

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
1.	Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и	ПК-1.1 Разрабатывает модели бизнес-процессов заказчика	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет

		бизнес-процессы		
2.	Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.8 Организует репозиторий хранения данных о создании (модификации) и вводе ИС в эксплуатацию ПК-1.9 Создание пользовательской документации к ИС	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет
3.	Тема 3. Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.1 Разрабатывает драйверы устройств ПК-3.2 Разрабатывает компиляторы, загрузчики, сборщики	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет
4.	Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.3 Разрабатывает системные утилиты ПК-3.4. Создает инструментальные	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенции, характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе итоговой аттестации.

Дисциплина «Криптографические методы защиты информации» является промежуточным этапом комплекса дисциплин, в ходе изучения которых у студентов формируются компетенции ПК-1, ПК-3.

Формирования компетенции ПК-1 начинается с изучения дисциплины «Технология кроссплатформенного программирования», «Методы и средства проектирования информационных систем и технологий», учебная практика: технологическая практика.

Формирования компетенции ПК-3 начинается с изучения дисциплины «Базы данных», «Информационная безопасность», «Инструментальные

средства информационных систем», учебная практика: технологическая практика.

Завершается работа по формированию у студентов указанных компетенций в ходе «Преддипломной практики» и подготовке и сдаче государственного экзамена.

Итоговая оценка сформированности компетенций ПК-1, ПК-3 определяется в период подготовки и сдачи государственного экзамена.

В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования ПК-1, ПК-3 при изучении дисциплины Б1.Д(М).В.14 «Криптографические методы защиты информации» является последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение студентами необходимыми дескрипторами (составляющими) компетенций. Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет.

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

8.2.1. Контрольные вопросы по темам (разделам) для опроса на занятиях

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции	Наименование оценочного средства
1.	Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1 Разрабатывает модели бизнес-процессов заказчика	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет
2.	Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы	ПК-1. Способен выполнять работы и управление работами по созданию	ПК-1.8 Организует репозиторий хранения данных о создании	Опрос, реферат, программы, презентации, ргр, курсовая

	аутентификации пользователей. Модели безопасности основных операционных систем.	(модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	(модификации) и вводе ИС в эксплуатацию ПК-1.9 Создание пользовательской документации к ИС	работа, зачет
3.	Тема 3. Администрирование сетей. Криптографические методы защиты информации в сетях. Многоуровневая защита корпоративных сетей.	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.1 Разрабатывает драйверы устройств ПК-3.2 Разрабатывает компиляторы, загрузчики, сборщики	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет
4.	Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.3 Разрабатывает системные утилиты ПК-3.4. Создает инструментальные	Опрос, реферат, программы, презентации, ргр, курсовая работа, зачет

Шкала оценивания ответов на вопросы

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает ответ на каждый теоретический вопрос, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«Хорошо»	Обучающийся в целом раскрывает теоретические вопросы, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает теоретические вопросы и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.
«Неудовлетворительно»	Обучающийся не знает ответов на поставленные теоретические вопросы.

8.2.2. Темы для докладов

Раздел 1. Корректирующие коды

1. Оценка и выбор корректирующего кода для контроля достоверности информации.
2. Построение циклического кода с минимальным кодовым расстоянием.
3. Алгоритм определения количества вариантов ошибок, не обнаруживаемых циклическим кодом.
4. Алгоритм построения кода Плоткина.

5. Алгоритм построения интерактивного кода.
6. Алгоритм построения кода Макдональда.
7. Алгоритм построения мажоритарного циклического кода.

Раздел 2. Современные симметричные криптосистемы

1. Американский стандарт шифрования данных DES.
2. Алгоритм шифрования данных IDEA.
3. Отечественный стандарт шифрования данных ГОСТ 28147–89.
4. Алгоритм построения криптосистемы Хилла.
5. Алгоритм шифрования информации методом гаммирования для симметричных систем.
6. Алгоритм шифрования информации методом Вернама для симметричных систем.
7. Обзор методов генерации, хранения и распространения криптографических ключей.

Раздел 3. Защита в операционных системах

1. Защита в операционной системе UNIX.
2. Защита в операционной системе Windows NT.
3. Защита в операционной системе IBM OS/390.
4. Методы и средства защиты от удаленных атак через сеть Internet.

Раздел 4. Ассиметричные криптосистемы

1. Схема шифрования Полига-Хеллмана.
2. Схема шифрования Эль-Гамаля.
3. Алгоритм цифровой подписи RSA.
4. Алгоритм цифровой подписи Эль-Гамаля.
5. Обзор методов и средств защиты от удаленных атак через сеть Internet.
6. Криптографические методы защиты информации в электронных платежных системах.
7. Обеспечение безопасности электронных платежей через сеть Internet.
8. Программная реализация однонаправленной хэш-функции на основе симметричных блочных алгоритмов.
9. Алгоритм цифровой подписи Эль-Гамаля для аутентификации электронных документов.
10. Реализация протокола идентификации с нулевой передачей знаний

Шкала оценивания

Шкала оценивания	Критерии оценивания
«Отлично»	Обучающийся глубоко и содержательно раскрывает тему доклада, не допустив ошибок. Ответ носит развернутый и исчерпывающий характер.
«Хорошо»	Обучающийся в целом раскрывает тему доклада, однако ответ хотя бы на один из них не носит развернутого и исчерпывающего характера.
«Удовлетворительно»	Обучающийся в целом раскрывает тему доклада и допускает ряд неточностей, фрагментарно раскрывает содержание теоретических вопросов или их раскрывает содержательно, но допуская значительные неточности.

«Неудовлетворительно»	Обучающийся не владеет выбранной темой

8.2.3. Оценочные средства остаточных знаний (тест)

1. Формы защиты информации:
- правовая;
- аналитическая;
- организационно-техническая;
- страховая.

2. Отметьте основные симптомы заражения системы вирусами:
- уменьшение объёма системной памяти и свободного места на диске без видимых причин;
- периодическое мерцание экрана;
- изменение длины файлов и даты создания;
- замедление работы программ, зависание и перезагрузка.

3. В необходимый минимум средств защиты от вирусов входит:
- архивирование;
- выходной контроль;
- профилактика;
- входной контроль.

4. Выделите три наиболее важных метода защиты информации от ошибочных действий пользователя:
- установление специальных атрибутов файлов;
- автоматический запрос на подтверждение выполнения команды или операции;
- дублирование носителей информации;
- предоставление возможности отмены последнего действия;
- шифрование файлов.

5. FireWall — это
- это графический редактор;
- это почтовая программа;
- то же самое, что и Интернет браузер;
- то же самое, что и брандмауэр.

6. Основные типы систем обнаружения атак:
- локальные;
- программное;
- сетевые;
- аппаратные.

7. Основные условные части вируса:
- тело вируса;

- хвост вируса;
- голова вируса.

8. Выделите наиболее важные методы защиты информации от несанкционированного доступа:
- использование антивирусных программ;
- архивирование (создание резервных копий);
- использование специальных «электронных ключей»;
- установление паролей на доступ к информации;
- шифрование.

9. Основными математическими задачами, лежащими в основе асимметричных криптосистем, являются:
- задача поиска «больших» простых чисел;
- задача поиска неприводимых многочленов в поле Галуа;
- задача дискретного логарифмирования;
- задача факторизации.

10. Методы коррекции ошибок:
- избыточное кодирование;
- дублирование передачи;
- шифрование;
- чётность.

11. Показателями безопасности информации являются:
- вероятность предотвращения угрозы;
- время, необходимое на взлом защиты информации;
- время, в течение которого обеспечивается определённый уровень безопасности;
- вероятность возникновения угрозы информационной безопасности.

12. Утечка информации по техническим каналам реализуется в результате:
- перехвата различного рода полей и сигналов;
- подслушивания конфиденциальных разговоров и акустических сигналов;
- наблюдения за источниками информации;
- недостаточной организацией защиты информации.

13. Виды каналов утечки информации:
- субъективные;
- технические;
- объективные;
- материально-вещественные.

14. Secure Sockets Layer:
- не может использовать шифрование с открытым ключом;

- это не протокол, а программа;
- обеспечивает безопасную передачу данных;
- не использует шифрование данных.

15. Расставьте в правильной последовательности основные действия (фазы), выполняемые компьютерным вирусом:
- заражение;
- маскировка;
- блокирование программ;
- проявление;
- размножение.

16. Виды уязвимостей:
- постоянная;
- субъективная;
- случайная;
- объективная.

17. Задачи, поставленные в рамках концепции национальной безопасности:
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий;
- совершенствование информационной структуры;
- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями её распространения;
- ускорение развития новых информационных технологий и их широкое распространение.

18. Признаки, определяющие класс вирусов:
- степень вредоносности;
- способ заражения;
- возможности;
- среда обитания.

19. Перечислите параметры, по которым можно классифицировать компьютерные вирусы:
- степень полезности;
- способ заражения среды обитания;
- степень опасности;
- объём программы;
- среда обитания.

20. Какие из перечисленных групп методов непосредственно связаны с защитой обрабатываемых данных:
- инженерно-технические;
- технические;

- аппаратно-программные;
- административные.

21. Что подразумевается под термином аутентичность информации?
- целостность информации;
- конфиденциальность;
- невозможность отказа от авторства;
- доступность информации;
- подлинность авторства.

22. Какой ключ доступен всем для проверки цифровой подписи под документом?
- закрытый;
- открытый;
- внутренний;
- приватный.

23.Как называется наука о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации?
- авторское право;
- Криптографические методы защиты информации;
- криптоанализ;
- криптография;
- матанализ.

24. Что является ключом в шифре Скитала?
- длина ленты;
- диаметр барабана.

25. В человеко-компьютерных системах необходимо обеспечивать защиту информации от следующих угроз:
- сбоев оборудования;
- преднамеренного искажения;
- резервного копирования;
- случайной потери или изменения;
- санкционированного просмотра.

26.По принципу Керкгоффа криптографическая стойкость шифра целиком определяется…
- его сложностью;
- временем шифрования;
- секретностью ключа;
- длиной ключа.

27. Электронно – цифровая подпись (ЭЦП) документа формируется на основе:
- специального вспомогательного документа;
- сторонних данных;
- перестановки элементов ключа.

28. Электронно – цифровая подпись устанавливает _____информации.
- непротиворечивость;
- целостность;
- противоречивость;
- тип.

29. Для защиты содержимого письма электронной почты от несанкционированного ознакомления используется:
- антивирусное средство;
- шифрование сообщения;
- электронно – цифровая подпись;
- межсетевой экран.

30. Сообщением в теории кодирования является:
– электрический импульс, распространяемый в канале связи телефонной линии;
– воспринятая, осознанная и ставшая личностно значимой информация;
– процесс переноса или копирования данных по некоторым признакам с одного места на другое с целью сортировки, формирования результирующих документов.

31. Наиболее защищёнными от несанкционированного доступа линиями связи на сегодня являются:
– оптоволоконные;
– электрические;
– инфракрасные;
– радио.

32.Принципиальным отличием межсетевых экранов (МЭ) от систем обнаружения атак (СОВ) является то, что:
– МЭ были разработаны для активной или пассивной защиты, а СОВ - для активного или пассивного обнаружения;
– МЭ работает только на сетевом уровне, а СОВ ещё и на физическом;
– МЭ были разработаны для активного или пассивного обнаружения, а СОВ - для активной или пассивной защиты;
– МЭ работает только на физическом уровне, а СОВ ещё и на сетевом.

33. Сжатый образ исходного текста используется:
– для создания электронно-цифровой подписи;
– как результат шифрования текста для его отправки по незащищённому каналу;

– в качестве ключа для шифрования текста;
– как открытый ключ в симметричных алгоритмах.

34. Сетевые черви – это:
– программы, которые не изменяют файлы на дисках, а распространяются в компьютерной сети, проникают в ОС, находят адреса других компьютеров или пользователей и рассылают по этим адресам свои копии;
– вредоносные программы, действие которых заключается в создании сбоев при питании компьютера от электрической сети;
– программы, распространяющиеся только при помощи электронной почты;
– программы, которые изменяют файлы на дисках.

35. Абсолютная защита персонального компьютера от сетевых атак возможна при:
– отсутствии соединения;
– установке межсетевого экрана;
– использовании лицензионного программного обеспечения;
– использовании новейших антивирусных средств.

36. Трояны - это:
– программы, которые не создают собственных копий, но преодолевают систему защиты компьютерной системы и оказывают вредоносное воздействие на её файловую систему;
– вредоносные программы, действие которых заключается в создании сбоев при питании компьютера от электрической сети;
– программы, распространяющиеся только при помощи электронной почты;
– программы, которые не изменяют файлы на дисках, а распространяются в компьютерной сети, проникают в ОС, находят адреса других компьютеров или пользователей и рассылают по этим адресам свои копии.

37.Организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач – это:
- уязвимость информации;
- автоматизированная система;
- качество информации.

38. Заражение компьютерными вирусами может произойти в процессе:
- работы с файлами;
- форматирования дискеты;
- выключения компьютера.

39. Что необходимо иметь для проверки на вирус жесткого диска?
- загрузочную программу;
- файл с антивирусной программой;

- дискету с антивирусной программой, защищенной от записи.

40. Какая программа не является антивирусной?
- AVP;
- Norton Antivirus;
- Defrag.

41. Вредоносная программа, которая распространяется в системах и сетях по линиям связи – это:
- «Троянский конь»;
- «Червь»;
- «Хамелеон».

42.Один из классов средств защиты информации, при котором различные электронные, электронно-механические и тому подобные устройства, схемно встраиваемые в аппаратуру АС или сопрягаемые с ней специально для решения задач защиты информации:
- аппаратные средства;
- организационные средства;
- физические средства.

43. Американский стандарт шифрования данных – это:
- FAT;
- ГОСТ;
- DES.

44.События или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой информации – это:
- угрозы безопасности информации;
- комплексная защита информации;
- изначально защищенная информация.

45.Процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленных статус ее защищенности – это:
- автоматизированная система;
- информационная безопасность;
- защита информации..

46. Какие программы не относятся к антивирусным?
- программы-фаги;
- программы сканирования;
- программы-детекторы.

47. Как происходит заражение «почтовым» вирусом?
- при открытии зараженного файла, присланного с письмом по e-mail;
- при подключении к почтовому серверу;
- при подключении к web-серверу, зараженному «почтовым» вирусом.

48. Отличительной характеристикой этого вируса является то, что пользователь обращается к этой программе считая ее полезной:
- «Троянский конь»;
- «Червь»;
- «Хамелеон».

49. Один из классов средств защиты информации, при котором специальные пакеты программ или отдельные программы, используемые для решения задач защиты:
- аппаратные средства;
- организационные средства;
- программные средства.

50. Возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации – это:
- автоматизированная система;
- качество информации;
- уязвимость информации.

51. Как обнаруживает вирус программа-ревизор?
- контролирует важные функции компьютера и пути возможного заражения;
- при открытии файла подсчитывает контрольные суммы и сравнивает их с данными, хранящимися в базе данных;
- отслеживает изменения загрузочных секторов дисков.

52. Заражению компьютерными вирусами могут подвергнуться:
- программы и документы;
- графические файлы;
- звуковые файлы.

53. Какие из перечисленных типов не относятся к категории вирусов?
- загрузочные вирусы;
- сетевые вирусы;
- туре-вирусы.

54. Эти вирусы «прячутся» не только от пользователей, но и от антивирусных программ, изменяют себя с помощью запутанных операций используя команды процессора:
- «Троянский конь»;

- «Червь»;
- «Хамелеон».

55. Один из классов средств защиты информации, при котором сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе:
- аппаратные средства;
- морально-этические средства;
- физические средства.

Шкала оценивания результатов тестирования

% верных решений (ответов)	Шкала оценивания
85 - 100	отлично
70 - 84	хорошо
50- 69	удовлетворительно
0 - 49	неудовлетворительно

8.2.4. Индивидуальные задания для выполнения расчетно-графической работы, курсовой работы (проекта)

РГР, КР и КП по дисциплине «Криптографические методы защиты информации» рабочей программой и учебным планом не предусмотрены.

8.2.5. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Вопросы (задания) для зачета:

1. Компьютерные вирусы. Их разновидности.
2. Антивирусные средства. Примеры антивирусных программ.
3. Понятие информационной безопасности.
4. Понятие конфиденциальности информации.
5. Понятие доступа к информации (санкционированный и несанкционированный доступ).
6. Понятия идентификация, аутентификация и авторизация.
7. Понятие угроза безопасности.
8. Понятие уязвимость системы (сети).
9. Понятие атаки на компьютерную систему.
10. Охарактеризуйте подходы к обеспечению компьютерной информации.
11. Перечислите основные и вспомогательные сервисы безопасности, дайте их классификацию.
12. Дайте характеристику групп требований к системе защиты.
13. «Фрагментарный» подход в обеспечении безопасности компьютерной системы.

14. «Комплексный» подход в обеспечении безопасности компьютерной системы.
15. В чем заключается политика безопасности компьютерной системы?
16. На чем основана «избирательная» политика безопасности?
17. На чем основана «полномочная» политика безопасности?
18. Понятие криптографии. Основные виды шифров.
19. Обобщенная схема криптосистемы. Понятия симметричной и асимметричной криптосистемы.
20. Перечислите основные алгоритмы криптографических преобразований.
21. Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях.
22. Как классифицируются средства криптографической защиты информации?
23. Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.
24. Перечислите основные комбинации, используемые при шифровании алгоритмом DES.
25. Перечислите основные режимы работы алгоритма DES.
26. Как обеспечивается криптостойкость асимметричных криптосистем?
27. Каково основное назначение хеш-функции?
28. Каковы основные принципы формирования хеш-функции?
29. Отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA.
30. Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия.
31. Современные приложения криптографии. Примеры.
32. Типичные атаки на операционную систему.
33. Понятие защищенной операционной системы.
34. Аппаратное обеспечение средств защиты операционной системы.
35. Проблемы безопасности IP-сетей.
36. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP.
37. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой операционной системе (ОС).
38. Какие элементы безопасности содержит ОС Windows 2000/XP/Vista?
39. Назовите элементы безопасности ОС UNIX?
40. Основные практические вопросы зашиты информации.
41. Программные средства защиты и уничтожения информации.
42. Основные принципы построения подсистемы информационной безопасности.
43. Этапы построения подсистемы информационной безопасности.
44. Общие принципы обеспечения информационной безопасности.
45. Средства обеспечения конфиденциальности данных.
46. Средства идентификации и аутентификации пользователей.

47. Приведите основные схемы идентификации и аутентификации пользователя.
48. Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными.
49. Средства аутентификации электронных данных.
50. Правовые последствия несанкционированного съема и использования конфиденциальной информации.
51. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.
52. Приведите классификацию систем защиты программного обеспечения.
53. Сравните основные технические методы и средства защиты программного обеспечения.
54. Назовите отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования.
55. Приведите определение понятий «протоколирование» и «аудит»
56. Назовите задачи, реализуемые протоколированием и аудитом.
57. Дайте характеристику задачи активного аудита.
58. Перечислите функции и компоненты сети VPN.
59. Классифицируйте VPN по способу технической реализации и архитектуре технического решения.
60. Каковы способы защиты информации при межсетевом взаимодействии?
61. Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

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

Основной целью проведения промежуточной аттестации является определение степени достижения целей по учебной дисциплине или ее разделам. Осуществляется это проверкой и оценкой уровня теоретической знаний, полученных обучающимися, умения применять их в решении практических задач, степени овладения обучающимися практическими навыками и умениями в объеме требований рабочей программы по дисциплине, а также их умение самостоятельно работать с учебной литературой.

Организация проведения промежуточной аттестации регламентирована «Положением об организации образовательного процесса в федеральном государственном автономном образовательном учреждении «Московский политехнический университет»

8.3.1. Показатели оценивания компетенций на различных этапах их формирования, достижение обучающимися планируемых результатов обучения по дисциплине

Код и наименование компетенции ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи

организационного управления и бизнес-процессы				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: Разработка модели бизнес-процессов заказчика	Обучающийся демонстрирует неполное соответствие следующих знаний: Разработка модели бизнес-процессов заказчика	Обучающийся демонстрирует частичное соответствие следующих знаний: Разработка модели бизнес-процессов заказчика	Обучающийся демонстрирует полное соответствие следующих знаний: Разработка модели бизнес-процессов заказчика
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять: Разрабатывать базы данных ИС	Обучающийся демонстрирует неполное соответствие следующих умений Разрабатывать базы данных ИС	Обучающийся демонстрирует частичное соответствие следующих умений: Разрабатывать базы данных ИС	Обучающийся демонстрирует полное соответствие следующих умений: Разрабатывать базы данных ИС
владеть	Обучающийся не владеет или в недостаточной степени владеет: технологиями программирования, технологиями модульного тестирования ИС (верификации)	Обучающийся владеет в неполном объеме и проявляет недостаточность владения навыками работы технологиями программирования технологиями модульного тестирования ИС (верификации)	Обучающимся допускаются незначительные ошибки, неточности, затруднения, частично владеет навыками работы технологиями программирования технологиями модульного тестирования ИС (верификации)	Обучающийся свободно применяет полученные навыки, в полном объеме владеет навыками работы технологиями программирования технологиями модульного тестирования ИС (верификации)

Код и наименование компетенции ПК-3. Способен разрабатывать компоненты системных программных продуктов				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: Создание инструментальные средства программирования	Обучающийся демонстрирует неполное соответствие следующих знаний: Создание инструментальные средства программирования	Обучающийся демонстрирует частичное соответствие следующих знаний: Создание инструментальные средства программирования	Обучающийся демонстрирует полное соответствие следующих знаний: Создание инструментальные средства программирования
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять: Разработкф компиляторы, загрузчики, сборщики	Обучающийся демонстрирует неполное соответствие следующих умений: Разработка компиляторы, загрузчики, сборщики	Обучающийся демонстрирует частичное соответствие следующих умений: Разработка компиляторы, загрузчики, сборщики	Обучающийся демонстрирует полное соответствие следующих умений: Разработка компиляторы, загрузчики, сборщики
владеть	Обучающийся не владеет или в недостаточной степени владеет: Разработкой системные утилиты	Обучающийся владеет в неполном объеме и проявляет недостаточность владения навыками работы Разработкой системные утилиты	Обучающимся допускаются незначительные ошибки, неточности, затруднения, частично владеет навыками работы Разработкой системные	Обучающийся свободно применяет полученные навыки, в полном объеме владеет навыками работы Разработкой системные утилиты

			утилиты	

8.3.2. Методика оценивания результатов промежуточной аттестации

Показателями оценивания компетенций на этапе промежуточной аттестации по дисциплине «Криптографические методы защиты информации» являются результаты обучения по дисциплине.

Оценочный лист результатов обучения по дисциплине

Код компетенции	Знания	Умения	Навыки	Уровень сформированности компетенции на данном этапе / оценка
ПК-3	- сущность и значение информации в развитии в развитии современного информационного общества; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности.	- выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности. -применять математические методы, вычислительную технику для решения практических задач; - анализировать и выбирать методы и средства обеспечения информационной безопасности.	численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; - элементами функционального анализа; - библиотечно-библиографическими знаниями; - методами и средства обеспечения информационной безопасности.	

ПК-1	- стандартные задачи профессиональной деятельности; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - понятия конфиденциальной информации, персональных данных и государственной тайны.	-применять математические методы, вычислительную технику для решения практических задач; -анализировать и выбирать методы и средства обеспечения информационной безопасности.	-элементами функционального анализа; -библиотечно-библиографическими знаниями.	
Оценка по дисциплине (среднее арифметическое)				

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, навыки).

Оценка «зачтено» выставляется, если среднее арифметическое находится в интервале от 2,4 до 5,0. Оценка «не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

Оценка «отлично» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0. Оценка «хорошо» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4. Оценка «удовлетворительно» выставляется, если среднее арифметическое находится в

интервале от 2,5 до 3,4. Оценка «неудовлетворительно» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

Промежуточная аттестация обучающихся в форме зачет проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по дисциплине «Криптографические методы защиты информации», при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «зачтено», или «не зачтено».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков по этапам (уровням) сформированности компетенций, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

9. Электронная информационно-образовательная среда

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационно-образовательной среде Чебоксарского института (филиала) Московского политехнического университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории филиала, так и вне ее.

Электронная информационно-образовательная среда – совокупность информационных и телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ в полном объёме независимо от места нахождения обучающихся.

Электронная информационно-образовательная среда обеспечивает:

а) доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

б) формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы;

в) фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы бакалавриата;

г) проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

д) взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих.

Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

Основными составляющими ЭИОС филиала являются:

а) сайт института в сети Интернет, расположенный по адресу www.polytech21.ru, https://chebpolytech.ru/ который обеспечивает:

- доступ обучающихся к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем, электронным информационным и образовательным ресурсам, указанных в рабочих программах (разделы сайта «Сведения об образовательной организации»);

- информирование обучающихся обо всех изменениях учебного процесса (новостная лента сайта, лента анонсов);

- взаимодействие между участниками образовательного процесса (подразделы сайта «Задать вопрос директору»);

б) официальные электронные адреса подразделений и сотрудников института с Яндекс-доменом @polytech21.ru (список контактных данных подразделений Филиала размещен на официальном сайте Филиала в разделе «Контакты», списки контактных официальных электронных данных преподавателей размещены в подразделах «Кафедры») обеспечивают взаимодействие между участниками образовательного процесса;

в) личный кабинет обучающегося (портфолио) (вход в личный кабинет размещен на официальном сайте Филиала в разделе «Студенту» подразделе «Электронная информационно-образовательная среда») включает в себя портфолио студента, электронные ведомости, рейтинг студентов и обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися,

- формирование электронного портфолио обучающегося, в том числе с сохранение работ обучающегося, рецензий и оценок на эти работы,

г) электронные библиотеки, включающие электронные каталоги, полнотекстовые документы и обеспечивающие доступ к учебно-методическим материалам, выпускным квалификационным работам и т.д.:

Чебоксарского института (филиала) - «ИРБИС»

д) электронно-библиотечные системы (ЭБС), включающие электронный каталог и полнотекстовые документы:

- «ЛАНЬ» -www.e.lanbook.com

- Образовательная платформа Юрайт -https://urait.ru

е) платформа цифрового образования Политеха - https://lms.mospolytech.ru/

ж) система «Антиплагиат» -https://www.antiplagiat.ru/

з) система электронного документооборота DIRECTUM Standard — обеспечивает документооборот между Филиалом и Университетом;

и) система «1С Управление ВУЗом Электронный деканат» (Московский политехнический университет) обеспечивает фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися;

к) система «POLYTECH systems» обеспечивает информационное, документальное автоматизированное сопровождение образовательного процесса;

л) система «Абитуриент» обеспечивает документальное автоматизированное сопровождение работы приемной комиссии.

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

Основная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247.

Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290.
2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее

образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132.

Периодика

Системы управления и информационные технологии: научный журнал - URL: http://sbook.ru/suit/- Текст : электронный

10. Профессиональные базы данных и информационно-справочные системы

Профессиональная база данных и информационно-справочные системы	Информация о праве собственности (реквизиты договора)
Университетская информационная система РОССИЯ https://uisrussia.msu.ru/	Тематическая электронная библиотека и база для прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права. свободный доступ
научная электронная библиотека Elibrary http://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научно-технических журналов, из которых более 4800 журналов в открытом доступе свободный доступ
сайт Института научной информации по общественным наукам РАН. http://www.inion.ru	Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объём массивов составляет более 3 млн. 500 тыс. записей (данные на 1 января 2012 г.). Ежегодный прирост — около 100 тыс. записей. В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языках, поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифром хранения и ссылками на полные тексты источников из Научной электронной библиотеки.
Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru	Федеральный портал «Российское образование» – уникальный интернет-ресурс в сфере образования и науки. Ежедневно публикует самые актуальные новости,

	анонсы событий, информационные материалы для широкого круга читателей. Еженедельно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными, репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.

12. Программное обеспечение (лицензионное и свободно распространяемое), используемое при осуществлении образовательного процесса

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
№ **219б** Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей)	1С:Предприятие 8. Комплект для обучения	договор № 08/10/2014-0731
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года. Band S: 150-249	Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.3К/21 от 24.12.2021 до 31.12.2023
	Google Chrome	Свободное распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic(Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Zoom	свободно распространяемое программное обеспечение (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	1С:Предприятие 8. Комплект для обучения	договор № 08/10/2014-0731
№ **206б** Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года. Band S: 150-249	Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.3К/21 от 24.12.2021 до 31.12.2023
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	MS Windows 10 Pro	договор № 392_469.223.3К/19 от 17.12.19 (бессрочная лицензия)

определяется в рабочих программах дисциплин (модулей)	Microsoft Office Standard 2019(Microsoft DreamSpark Premium Electronic Software Delivery Academic(Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	КОМПАС-3D V16 и V17	договор № НП-16-00283 от 1.12.2016 (бессрочная лицензия)
	MathCADv.15	Сублиц.договор №39331/МОС2286 от 6.05.2013) номер лицензии-42661846 от 30.08.2007) (бессрочная лицензия)
	SimInTech	Отечественное программное обеспечение
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	AdobeFlashPlayer	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Visual Studio 2019	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Python 3.7	свободно распространяемое программное обеспечение (бессрочная лицензия)
	PascalABC	свободно распространяемое программное обеспечение (бессрочная лицензия)
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)
№ 112б Помещение для самостоятельной работы обучающихся	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года. Band S: 150-249	Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.ЗК/21 от 24.12.2021 до 31.12.2023
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Гарант	Договор № 735_480.2233К/20 от 15.12.2020
	Yandex браузер	свободно распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic(Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Zoom	свободно распространяемое программное обеспечение (бессрочная лицензия)

13. Материально-техническое обеспечение дисциплины

Дисциплины

Тип и номер помещения	Перечень основного оборудования и технических средств обучения
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) 219б Кабинет систем управления (Чебоксары, ул. К.Маркса, д.60)	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: компьютерная техника; мультимедийное оборудование (проектор, экран)
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Компьютерный класс №206б (Чебоксары, ул. К.Маркса, д.60)	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: компьютерная техника
Помещение для самостоятельной работы обучающихся № 112б (г. Чебоксары, ул. К.Маркса. 60)	Оборудование: комплект мебели для учебного процесса; Технические средства обучения: компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Филиала

Методические указания для занятий лекционного типа

В ходе лекционных занятий обучающемуся необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации.

Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из основной и дополнительной литературы, рекомендованной преподавателем и предусмотренной учебной программой дисциплины.

Методические указания для занятий семинарского (практического) типа.

Практические занятия позволяют развивать у обучающегося творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор основной и дополнительной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку к занятию, которая начинается с изучения основной и дополнительной литературы. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. Далее следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие или по теме, вынесенной на дискуссию (круглый стол), продумать примеры с целью обеспечения тесной связи изучаемой темы с реальной жизнью.

Готовясь к докладу или выступлению в рамках интерактивной формы (дискуссия, круглый стол), при необходимости следует обратиться за помощью к преподавателю.

Методические указания к самостоятельной работе.

Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала по учебной дисциплине может выполняться в библиотеке университета, учебных кабинетах, компьютерных классах, а также в домашних условиях. Содержание и количество самостоятельной работы обучающегося определяется учебной программой дисциплины, методическими материалами, практическими заданиями и указаниями преподавателя.

Самостоятельная работа в аудиторное время может включать:

1) конспектирование (составление тезисов) лекций;
2) выполнение контрольных работ;
3) решение задач;
4) работу со справочной и методической литературой;
5) работу с нормативными правовыми актами;
6) выступления с докладами, сообщениями на семинарских занятиях;
7) защиту выполненных работ;
8) участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;
9) участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;
10) участие в тестировании и др.

Самостоятельная работа во внеаудиторное время может состоять из:

1) повторения лекционного материала;
2) подготовки к практическим занятиям;
3) изучения учебной и научной литературы;

4) изучения нормативных правовых актов (в т.ч. в электронных базах данных);

5) решения задач, и иных практических заданий

6) подготовки к контрольным работам, тестированию и т.д.;

7) подготовки к практическим занятиям устных докладов (сообщений);

8) подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;

9) выполнения курсовых работ, предусмотренных учебным планом;

10) выполнения выпускных квалификационных работ и др.

11) выделения наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на консультациях.

12) проведения самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

Текущий контроль осуществляется в форме устных, тестовых опросов, докладов, творческих заданий.

В случае пропусков занятий, наличия индивидуального графика обучения и для закрепления практических навыков студентам могут быть выданы типовые индивидуальные задания, которые должны быть сданы в установленный преподавателем срок.

15. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение по дисциплине « Криптографические методы защиты информации» инвалидов и лиц с ограниченными возможностями здоровья (далее ОВЗ) осуществляется преподавателем с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Для студентов с нарушениями опорно-двигательной функции и с ОВЗ по слуху предусматривается сопровождение лекций и практических занятий мультимедийными средствами, раздаточным материалом.

Для студентов с ОВЗ по зрению предусматривается применение технических средств усиления остаточного зрения, а также предусмотрена возможность разработки аудиоматериалов.

По дисциплине « Криптографические методы защиты информации» обучение инвалидов и лиц с ограниченными возможностями здоровья может осуществляться как в аудитории, так и с использованием электронной информационно-образовательной среды, образовательного портала и электронной почты.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ

рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры, протокол № 10 от «10» апреля 2021 г.

Внесены дополнения и изменения в части актуализации лицензионного программного обеспечение, используемое при осуществлении образовательного процесса по данной дисциплины, а так же современных профессиональных баз данных и информационных справочных системах.

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры, протокол № 10 от «14» мая 2022 г.

Внесены дополнения и изменения в части актуализации лицензионного программного обеспечение, используемое при осуществлении образовательного процесса по данной дисциплины, а так же современных профессиональных баз данных и информационных справочных системах, актуализации тем для самостоятельной работы, актуализации вопросов для подготовки к промежуточной аттестации, актуализации перечня основной и дополнительной учебной литературы.

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры, протокол № 6 от «04» марта 2023г.

Внесены дополнения и изменения в части актуализации лицензионного программного обеспечение, используемое при осуществлении образовательного процесса по данной дисциплины, а так же современных профессиональных баз данных и информационных справочных системах, актуализации электронно-библиотечных систем.

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры, протокол № 8 от «16» марта 2024г.

Внесены дополнения и изменения в части актуализации лицензионного программного обеспечение, используемое при осуществлении образовательного процесса по данной дисциплины, а так же современных профессиональных баз данных и информационных справочных системах, актуализации электронно-библиотечных систем.