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 и систем управления

УТВЕРЖДАЮ
Директор филиала
_____А.В. Агафонов
"27" мая 2026г.

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**
Год начала обучения	**2026**

Чебоксары, 2026

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

Автор Пикина Наталия Евгеньевна, кандидат педагогических наук, доцент кафедры информационных технологий и систем управления

(указать ФИО, ученую степень, ученое звание или должность)

Программа одобрена на заседании кафедры Информационных технологий и систем управления (протокол № 9 от 22.05.2026 г.).

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:

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.

Для достижения целей дисциплины необходимо решить следующую *основную задачу* – сформировать у обучающихся теоретические знания и практические навыки, необходимые для:

– получение студентами знаний о теоретических основах криптографии;

– 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 Министерством труда и социальной защиты Российской Федерации от 18.11.2013 № 679н (зарегистрирован в Министерстве труда и социальной защиты Российской Федерации от 18	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
декабря 2013 г. №30635)						
06.028 Системный программист Профессиональный стандарт «Системный программист», утв. Приказом Министерством труда и социальной защиты РФ от 29 сентября 2020 года N 678н	A	Разработка компонентов системных программных продуктов	6	Разработка драйверов устройств	A/01.6	6
			6	Разработка компиляторов, загрузчиков, сборщиков	A/02.6	6
				Разработка системных утилит	A/03.6	6
				Создание инструментальных средств программирования	A/04.6	6
06.015 Специалист по информационным системам Профессиональный стандарт «Специалист по информационным системам», утв. приказом Министерством труда и социальной защиты РФ 18 ноября 2014 г. №896н	C	Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	6	Разработка модели бизнес-процессов заказчика	C/08.6	6
				Выявление требований к ИС	C/11.6	6
				Анализ требований	C/12.6	6
				Разработка архитектуры ИС	C/14.6	6
				Проектирование и дизайн ИС	C/16.6	6
				Разработка баз данных ИС	C/17.6	6
				Организационное и технологическое обеспечение кодирования на языках программирования	C/18.6	6
				Организационное и технологическое обеспечение модульного тестирования ИС (верификации)	C/19.6	6
				Создание пользовательской документации к	C/22.6	6

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
				ИС		
				Организация репозитория хранения данных о создании (модификации) и вводе ИС в эксплуатацию	C/40.6	6

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**
Создание (модификация) и сопровождение ИС	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1 Знать: модели бизнес-процессов заказчика, требования к ИС, архитектуру ИС	*на уровне знаний:* знать стандартные задачи профессиональной деятельности; *на уровне умений:* уметь применять математические методы, вычислительную технику для решения практических задач; *на уровне навыков:* владеть практическими навыками поиска и обработки информации.
		ПК-1.2 Уметь: проектировать ИС, разрабатывать базы данных ИС, использовать технологии программирования	*на уровне знаний:* знать стандартные задачи профессиональной деятельности; современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; *на уровне умений:* уметь применять современные тенденции развития информатики и

			вычислительной техники, *на уровне навыков:* владеть практическими навыками поиска и анализа и синтеза информации.
		ПК-1.3 Владеть: технологиями модульного Тестирования ИС (верификации), организацией репозиторий хранения данных	*на уровне знаний:* знать основы информационно-коммуникационных технологий; понятия конфиденциальной информации, персональных данных и государственной тайны. *на уровне умений:* уметь анализировать и выбирать методы и средства обеспечения информационной безопасности. *на уровне навыков:* владеть элементами функционального анализа; библиотечно-библиографическими знаниями.
Разработка, отладка, модификация и поддержка системного программного обеспечения	ПК-3. Способен разрабатывать компоненты системных программных продуктов	ПК-3.1 Разрабатывает драйверы устройств	*на уровне знаний:* знать сущность и значение информации в развитии в развитии современного информационного общества; *на уровне умений:* уметь использовать современные тенденций в области информатики и вычислительной техники; *на уровне навыков:* владеть навыками анализа и выбора методов и инструментов для обеспечения информационной безопасности.

		ПК-3.2 Разрабатывает компиляторы, загрузчики, сборщики	*на уровне знаний:* знать основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; *на уровне умений:* уметь применять информационно-коммуникационных технологии *на уровне навыков:* владеть оценкой рисков, разработку стратегий защиты, применение современных технологий защиты данных, а также мониторинг и аудит информационных систем.
		ПК-3.3 Разрабатывает системные утилиты	*на уровне знаний:* знать виды угроз, возникающие в процессе информационной деятельности; *на уровне умений:* уметь выбирать актуальные информационные ресурсы и источники знаний в электронной среде, а также уметь выявлять угрозы информационной безопасности. *на уровне навыков:* владеть развить навыки их правильного применения для защиты данных и систем от возможных угроз и атак
		ПК-3.4. Создает инструментальные средства программирования	*на уровне знаний:* знать методы и средства обеспечения информационной безопасности объектов профессиональной деятельности. *на уровне умений:* уметь выбирать необходимые информационные ресурсы и источники знаний в электронной среде -

			выявлять угрозы информационной безопасности. *на уровне навыков:* владеть методами и средства обеспечения информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.Д(М).В.ДВ.1.1 «Криптографические методы защиты информации» реализуется в рамках вариативной части Блока 1 «Элективные дисциплины (модули)» программы бакалавриата.

Дисциплина «Криптографические методы защиты информации» преподается обучающимся по очной форме обучения – в 4-м семестре, по заочной форме – в 6-м 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 Перспективы развития информатики и вычислительной техники, Введение в информатику, Учебная практика: ознакомительная практика, Объектно-ориентированное программирование, Программирование для мобильных устройств, Структуры и алгоритмы обработки данных и является предшествующей для изучения дисциплин Учебная практика: научно-исследовательская работа (получение первичных навыков научно-исследовательской работы), Учебная практика: технологическая (проектно-технологическая) практика, Методы и средства проектирования информационных систем и технологий, Микропроцессорные устройства систем управления, Интернет-технологии, Интернет-программирование, Функциональное и логическое программирование, ЭВМ и периферийные устройства, Операционные системы, Системное программирование, Автоматизированные информационно-управляющие системы, Производственная практика: преддипломная практика, Государственная итоговая аттестация: подготовка к сдаче и сдача государственного экзамена, Государственная итоговая аттестация: выполнение и защита выпускной квалификационной работы.

Формой промежуточной аттестации знаний обучаемых по очной форме обучения является зачет во 4-м семестре, по заочной форме зачет в 6-м семестре.

3. Объем дисциплины

очная форма обучения:

Вид учебной работы по дисциплине	**Всего в з.е. и часах**	**Семестр 4 в часах**

Общая трудоёмкость дисциплины	**3 з.е. -108 ак.час**	**108 ак.час**
Контактная работа - Аудиторные занятия	**36**	**36**
Лекции	18	18
Лабораторные занятия	18	18
Семинары, практические занятия	-	-
Консультация	-	-
Самостоятельная работа	**72**	**72**
Курсовая работа (курсовой проект)	-	-
Вид промежуточной аттестации	зачет	зачет

заочная форма обучения:

Вид учебной работы по дисциплине	**Всего в з.е. и часах**	**Семестр 6 в часах**
Общая трудоёмкость дисциплины	**3 з.е. -108 ак.час**	**108 ак.час**
Контактная работа - Аудиторные занятия	**8**	**8**
Лекции	4	4
Лабораторные занятия	4	4
Семинары, практические занятия	-	-
Консультация	-	-
Самостоятельная работа	**96**	**96**
Курсовая работа (курсовой проект)	-	-
Вид промежуточной аттестации	зачет – 4 часа	зачет – 4 часа

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

4.1. Учебно-тематический план

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	-	18	ПК-1.1, ПК-1.2, ПК-1.3, 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	-	18	ПК-1.1, ПК-1.2, ПК-1.3, 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	-	18	ПК-1.1, ПК-1.2, ПК-1.3, 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	6	6	-	18	ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Консультация	-			-	ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Курсовая работа (курсовой проект)	-				ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Контроль (зачет)	-				ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
ИТОГО	**36**			**72**	

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	2	-	-	24	ПК-1.1, ПК-1.2, ПК-1.3, 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.	-	2	-	24	ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	2	-	-	24	ПК-1.1, ПК-1.2, ПК-1.3, 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	-	2	-	24	ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4

Консультация	-	-	ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Курсовая работа (курсовой проект)	-		ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
Контроль (зачет)	-		ПК-1.1, ПК-1.2, ПК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-3.4
ИТОГО	**8**	**96**	

4.2. Содержание дисциплины

Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности

Определение криптографии и её роль в защите информации.

Основные криптографические термины: шифрование, дешифрование, ключи, хэширование, аутентификация.

Источники угроз безопасности: внутренние и внешние угрозы.

Виды атак на информацию: перехват, подмена данных, повторные атаки, атаки на отказ в обслуживании.

Риски безопасности: угрозы конфиденциальности, целостности и доступности информации.

Основные формы атак: пассивные, активные, с использованием уязвимостей, социальной инженерии.

Роль политики безопасности и её элементов: классификация информации, разграничение доступа, управление рисками.

Международные стандарты безопасности: ISO/IEC 27001, FIPS, NIST, и их влияние на криптографическую практику.

Принципы создания и реализации безопасных информационных систем.

Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.

Криптографические модели защиты информации: симметричное и асимметричное шифрование, цифровые подписи, хэш-функции.

Алгоритмы шифрования:

- Симметричные алгоритмы: DES, AES, RC4 и их особенности.
- Асимметричные алгоритмы: RSA, DSA, Diffie-Hellman.
- Применение и ограничения алгоритмов шифрования в реальных системах.

Алгоритмы аутентификации пользователей:

- Парольные и ключевые методы аутентификации.
- Многофакторная аутентификация.
- Протоколы аутентификации: Kerberos, LDAP.

- Модели безопасности в операционных системах:
  - Основы безопасности в ОС: контролируемый доступ, права пользователей, учет событий.
  - Модели безопасности: модели Бэлла-ЛаПадулы (Bell-LaPadula), Биби-Таненбаума (Biba), Clark-Wilson.
  - Защита данных в операционных системах: шифрование файлов, защиты от утечек данных.

Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.

Основы администрирования сетей и управления безопасностью.

Сетевые угрозы и атаки: атаки на уровень транспортного, сетевого и канала передачи.

Протоколы безопасности в сетях: VPN, SSL/TLS, IPSec.

- Методы защиты информации в сетях:
  - Шифрование трафика, защита каналов связи.
  - Защита от DoS и DDoS-атак, межсетевые экраны (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS).
  - Протоколы безопасной передачи данных: SSH, HTTPS, SNMPv3.

- Многоуровневая защита корпоративных сетей:
  - Сегментация сети, использование DMZ (демилитаризованной зоны).
  - Использование брандмауэров и шлюзов для защиты периметра сети.
  - Политики безопасности в корпоративных сетях: управление доступом, мониторинг и аудит.

Защита беспроводных сетей: Wi-Fi безопасность, WPA2/WPA3, использование VPN.

Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации

- Требования к системам защиты информации:
  - Конфиденциальность, целостность, доступность информации.
  - Контроль доступа, защита от утечек данных, резервное копирование.
  - Принципы создания безопасных информационных систем на уровне организации.

- Современные средства безопасности предприятия:
  - Антивирусные программы, средства мониторинга и управления инцидентами.
  - Инструменты защиты данных: шифрование, токенизация, защита на уровне приложений.

~ Использование искусственного интеллекта и машинного обучения для предсказания и выявления угроз.

Направления развития средств безопасности:

~ Развитие облачных решений и защиты информации в облаке.

~ Автоматизация управления безопасностью: SIEM-системы, SOAR.

~ Развитие биометрических методов защиты и многофакторной аутентификации.

Правовые последствия несанкционированного доступа к информации:

~ Ответственность за нарушение прав на информацию в разных странах.

~ Законы о защите данных и киберпреступности (GDPR, Закон о кибербезопасности, США).

~ Влияние законодательства на организацию информационной безопасности и защиту персональных данных.

5. Учебно-методическое обеспечение самостоятельной работы студентов

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.

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.

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

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	1. Определение криптографии и её роль в защите информации. 2. Основные понятия: конфиденциальность, целостность, доступность. 3. Источники угроз и риски безопасности информации. 4. Формы атак на информацию: взлом, фишинг, DDoS, вирусы и др. 5. Политики безопасности: основные компоненты и их значение. 6. Стандарты безопасности информации: ISO/IEC 27001 и другие. 7. Оценка рисков в области безопасности информации. 8. Социальная инженерия как форма атаки: методы и примеры. 9. Роль образовательных программ в повышении безопасности. 10. Будущее защиты информации: новые угрозы и подходы.	Изучение литературы по основным понятиям криптографии и безопасности информации. Проведение сравнительного анализа возможных угроз для информации в разных сферах.
Тема 2.	1. Обзор криптографических моделей: симметричная и	Исследование методов

Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	асимметричная криптография. 2. Алгоритмы шифрования: DES, AES, RSA и их особенности. 3. Применение хэш-функций в криптографии: SHA-1, SHA-256 и другие. 4. Алгоритмы аутентификации: пароли, токены, биометрия. 5. Модели безопасности в операционных системах: Windows, Linux, macOS. 6. Влияние криптографических методов на безопасность операционных систем. 7. Примеры применения различных алгоритмов шифрования в реальных системах. 8. Роль сертификатов и PKI в аутентификации пользователей. 9. Соответствие стандартам безопасности алгоритмов шифрования. 10. Будущее криптографических методов: новые решения и подходы.	аутентификации пользователей и их эффективности. Проведение анализа моделей безопасности основных операционных систем. Просмотр видеоматериалов о современных криптографических методах.
Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	1. Основы администрирования сетей: задачи и инструменты. 2. Угрозы безопасности в сетях: типы и источники. 3. Методы защиты информации в сетях: шифрование, VPN, файрволы. 4. Многоуровневая защита корпоративных сетей: концепции и подходы. 5. Роль сетевых протоколов в безопасности информации. 6. Применение IDS и IPS в защите сетей. 7. Системы управления безопасностью информации (SIEM): функции и примеры. 8. Основные принципы проектирования безопасных сетей. 9. Обучение сотрудников безопасности в корпоративной среде. 10. Будущее сетевой безопасности: тренды и технологии.	Проведение анализа многоуровневой защиты корпоративных сетей. Исследование примеров успешного администрирования сетей с акцентом на безопасность.
Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	1. Основные требования к системам защиты информации. 2. Нормативные документы и стандарты в области защиты информации. 3. Направления развития средств безопасности: тенденции и инновации. 4. Роль технологий в обеспечении безопасности информации на предприятиях. 5. Правовые аспекты защиты информации: законы и регуляции. 6. Последствия несанкционированного доступа к информации: юридические и финансовые. 7. Примеры успешного внедрения систем защиты в компаниях. 8. Влияние GDPR и других регуляций на защиту	Исследование правовых последствий несанкционированного доступа к информации. Проведение анализа современных тенденций в области средств безопасности.

	информации. 9. Оценка угроз и оценка рисков в контексте правовых последствий. 10. Будущее систем защиты информации: новые подходы и вызовы.	

Шкала оценивания

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

6. Оценочные материалы (фонд оценочных средств) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. 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 бизнес-процессы	ПК-1.1 Знать: модели бизнес- процессов заказчика, требования к ИС, архитектуру ИС ПК-1.2 Уметь: проектировать ИС, разрабатывать базы данных ИС, использовать технологии Программирования ПК-1.3 Владеть: технологиями модульного тестированияИС	Опрос, доклад, реферат, тест, зачет

			(верификации), организацией репозиторий хранения данных	
		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	Опрос, доклад, реферат, тест, зачет
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-1.1 Знать: модели бизнес- процессов заказчика, требования к ИС, архитектуру ИС ПК-1.2 Уметь: проектировать ИС, разрабатывать базы данных ИС, использовать технологии Программирования ПК-1.3 Владеть: технологиями модульного тестированияИС (верификации), организацией репозиторий хранения данных	Опрос, доклад, реферат, тест, зачет
		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	Опрос, доклад, реферат, тест, зачет
3.	Тема 3. Администрирование сетей. Криптографические методы защиты информации в сетях.	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и	ПК-1.1 Знать: модели бизнес- процессов заказчика, требования к ИС, архитектуру ИС ПК-1.2 Уметь:	Опрос, доклад, реферат, тест, зачет

	Многоуровневая защита корпоративных сетей.	сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	проектировать ИС, разрабатывать базы данных ИС, использовать технологии Программирования ПК-1.3 Владеть: технологиями модульного тестированияИС (верификации), организацией репозиторий хранения данных	
		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	Опрос, доклад, реферат, тест, зачет
4.	Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	ПК-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-1.1 Знать: модели бизнес- процессов заказчика, требования к ИС, архитектуру ИС ПК-1.2 Уметь: проектировать ИС, разрабатывать базы данных ИС, использовать технологии Программирования ПК-1.3 Владеть: технологиями модульного тестированияИС (верификации), организацией репозиторий хранения данных	Опрос, доклад, реферат, тест, зачет
		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	Опрос, доклад, реферат, тест, зачет

			системные утилиты ПК-3.4. Создает инструментальные	

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 «Криптографические методы защиты информации».

Формирования компетенции ПК-3 начинается с изучения дисциплины «Перспективы развития информатики и вычислительной техники», «Введение в информатику», Учебная практика: ознакомительная практика, «Объектно-ориентированное программирование», «Программирование для мобильных устройств», «Структуры и алгоритмы обработки данных».

Завершается работа по формированию у студентов указанных компетенций в ходе изучения дисциплин Учебная практика: научно-исследовательская работа (получение первичных навыков научно-исследовательской работы), Учебная практика: технологическая (проектно-технологическая) практика, Методы и средства проектирования информационных систем и технологий, Микропроцессорные устройства систем управления, Интернет-технологии, Интернет-программирование, Функциональное и логическое программирование, ЭВМ и периферийные устройства, Операционные системы, Системное программирование, Автоматизированные информационно-управляющие системы, Производственная практика: преддипломная практика.

Итоговая оценка сформированности компетенций ПК-1, ПК-3 определяется в период Государственная итоговая аттестация: подготовка к сдаче и сдача государственного экзамена, Государственная итоговая аттестация: выполнение и защита выпускной квалификационной работы.

В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования ПК-1, ПК-3 при изучении дисциплины Б1.Д(М).В.ДВ.1.1 «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.

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

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

Тема (раздел)	Вопросы
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК-1 1. Основные понятия информационной безопасности. 2. Классификация угроз безопасности информации. 3. Источники угроз и уязвимости информационных систем. 4. Формы и методы атак на информационные ресурсы. 5. Принципы оценки рисков в информационной безопасности. 6. Методы построения моделей угроз. 7. Основные элементы системы управления информационной безопасностью. 8. Международные стандарты в области ИБ (ISO/IEC 27001 и др.). 9. Цели и задачи политики безопасности в организации. 10. Система управления рисками в информационной безопасности. ПК-3 11. Структура политики информационной безопасности. 12. Документирование и реализация политики ИБ. 13. Виды стандартов и нормативных документов в области ИБ. 14. Порядок разработки внутренней нормативной документации по ИБ. 15. Ответственность сотрудников за соблюдение политики безопасности. 16. Организация системы контроля за соблюдением политики ИБ. 17. Внутренний аудит политик безопасности. 18. Интеграция политики безопасности в бизнес-процессы. 19. Практика применения политики безопасности на предприятии. 20. Управление инцидентами в рамках политики безопасности.
Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	ПК-1 1. Структура криптографической модели защиты информации. 2. Симметричное и асимметричное шифрование. 3. Алгоритмы симметричного шифрования (AES, DES и др.). 4. Алгоритмы асимметричного шифрования (RSA, ElGamal и др.). 5. Хэш-функции и их применение в защите информации. 6. Электронная подпись как средство криптографической защиты. 7. Механизмы аутентификации пользователей в ИС. 8. Многофакторная аутентификация. 9. Реализация дискреционных и мандатных моделей безопасности. 10. Особенности реализации защиты в ОС Windows и Linux.

	ПК-3 11. Использование криптографических библиотек и средств в ИС. 12. Управление криптографическими ключами. 13. Реализация PKI (инфраструктуры открытых ключей). 14. Средства аппаратного шифрования. 15. Применение криптографических алгоритмов в системах документооборота. 16. Интеграция криптографической защиты в бизнес-приложения. 17. Практика построения защищенных каналов связи. 18. Использование токенов и смарт-карт в аутентификации. 19. Сравнительный анализ моделей безопасности операционных систем. 20. Использование сертифицированных СКЗИ в информационных системах.
Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	ПК-1 1. Роль администратора в обеспечении сетевой безопасности. 2. Протоколы защищенного взаимодействия в сетях (TLS, SSH и др.). 3. Принципы работы межсетевых экранов. 4. Использование NAT и VPN в защите сетевых соединений. 5. Методы обнаружения и предотвращения сетевых атак. 6. Система обнаружения вторжений (IDS) и предотвращения (IPS). 7. Реализация концепции Zero Trust в корпоративных сетях. 8. Принципы многоуровневой защиты сетей. 9. Аутентификация и авторизация в сетевых системах. 10. Сегментация и контроль доступа в сетевой инфраструктуре. ПК-3 11. Организация мониторинга событий безопасности в сети. 12. Построение защищённой архитектуры корпоративной сети. 13. Реализация разграничения доступа на уровне сети. 14. Интеграция SIEM-систем в инфраструктуру предприятия. 15. Защита беспроводных сетей и корпоративного Wi-Fi. 16. Безопасность облачных и гибридных сетевых решений. 17. Настройка и обновление сетевых устройств с учетом ИБ. 18. Организация резервного копирования и восстановления данных в сети. 19. Обработка инцидентов безопасности в сетевой инфраструктуре. 20. Управление сетевыми политиками безопасности.
Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	ПК-1 1. Общие требования к системам защиты информации. 2. Принципы сертификации средств защиты информации. 3. Уровни доверия и классификация ИС по уровню защищённости. 4. Методы оценки эффективности систем защиты. 5. Минимизация прав доступа и управление привилегиями. 6. Ответственность за нарушение режима конфиденциальности. 7. Последствия несанкционированного доступа к информации. 8. Порядок расследования инцидентов ИБ. 9. Организация внутреннего контроля системы защиты. 10. Оценка ущерба от реализации угроз. ПК-3 11. Нормативно-правовая база защиты информации в РФ.

	12. Организация процессов защиты информации на предприятии. 13. Аттестация объектов информатизации по требованиям ИБ. 14. Взаимодействие с контролирующими органами (ФСТЭК, ФСБ и др.). 15. Правовые аспекты обработки персональных данных. 16. Принципы построения безопасных корпоративных ИС. 17. Перспективы развития технологий защиты информации. 18. Соответствие требованиям стандартов ИБ (ГОСТ, ISO). 19. Разработка внутренней нормативной документации по ИБ. 20. Управление жизненным циклом информационной безопасности в организации.

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.

6.2.2. Темы для докладов

Тема (раздел)	Вопросы
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК1: 1. Введение в криптографию и её роль в защите информации 2. Типы атак на информацию: классификация и риски 3. Политики безопасности информации в организациях 4. Криптографические стандарты и их значение 5. Оценка рисков в защите информации ПК-3: 6. Риски и угрозы в защите информации на уровне государственных и корпоративных структур 7. Формы атак на информацию и методы защиты от них 8. Процесс разработки и внедрения стандартов безопасности 9. Влияние политик безопасности на организационные процессы 10. Стандарты защиты информации в цифровой эпохе
Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных	ПК1: 1. Основы криптографических моделей защиты информации 2. Алгоритмы симметричного шифрования: AES, DES, и их особенности 3. Алгоритмы асимметричного шифрования: RSA, Эль-Гамаль 4. Методы аутентификации пользователей: пароли, сертификаты 5. Модели безопасности в операционных системах (например,

операционных систем.	Windows, Linux) ПК-3: 6. Алгоритмы хэширования: MD5, SHA, их применение и уязвимости 7. Двухфакторная аутентификация и её реализация 8. Обзор современных методов криптографической защиты в операционных системах 9. Криптографические протоколы для безопасной аутентификации (SSL, TLS) 10. Риски и уязвимости криптографических моделей и алгоритмов
Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	ПК1: 1. Основы администрирования сетей и обеспечения их безопасности 2. Методы защиты данных в локальных и глобальных сетях 3. Сетевые угрозы и способы защиты от них 4. Протоколы безопасности для передачи данных в сети (IPSec, SSL) 5. Системы обнаружения и предотвращения вторжений (IDS/IPS) ПК-3: 6. Многоуровневая защита корпоративных сетей 7. Сегментация сети и её значение для безопасности 8. Защита информации в облачных вычислениях и виртуализация 9. Технологии VPN и их роль в защите информации 10. Инструменты мониторинга и управления безопасностью сети
Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	ПК1: 1. Основные требования к системам защиты информации на предприятиях 2. Роль систем защиты информации в обеспечении непрерывности бизнеса 3. Типы систем защиты информации и их характеристики 4. Основные принципы разработки средств защиты информации на предприятии 5. Влияние правовых норм на разработку систем защиты информации ПК-3: 6. Направления развития средств защиты информации в корпоративных сетях 7. Влияние технологий блокчейн на безопасность данных 8. Правовые последствия несанкционированного доступа к информации 9. Риски для бизнеса от утечек информации и их последствия 10. Роль внешних аудиторов в обеспечении безопасности данных

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

6.2.3. Оценочные средства остаточных знаний (тест)

ПК-1.

1. Какой из методов шифрования является симметричным?

1) RSA
2) AES
3) ECC
4) Diffie-Hellman

2. Что такое криптографический хэш?

1) Алгоритм шифрования
2) Метод получения уникального идентификатора данных
3) Метод генерации случайных чисел
4) Алгоритм для проверки подлинности сообщений

3. Какой тип атак используется для взлома паролей с помощью предварительно вычисленных хэш-значений?

1) Атака «грубой силы»
2) Атака по словарю
3) Атака с использованием радужных таблиц
4) Атака «человек посередине»

4. Какой алгоритм используется для шифрования данных в современных Wi-Fi сетях?

1) DES
2) AES
3) RC4
4) RSA

5. Какой механизм аутентификации используется в протоколе WPA2 для защиты Wi-Fi сетей?

1) ECDSA
2) TLS
3) PSK (Pre-Shared Key)
4) AES

6. Какой из перечисленных алгоритмов не является алгоритмом асимметричного шифрования?

1) RSA
2) ElGamal
3) AES
4) ECC

7. Какую функцию выполняет публичный ключ в асимметричной криптографии?

1) Шифрует данные
2) Дешифрует данные
3) Подписывает сообщения
4) Проверяет подписи

8. Как называется атака на систему, при которой пытаются подобрать секретный ключ методом «грубой силы»?

1) Атака с использованием радужных таблиц
2) Атака по словарю
3) Атака на основе шифра
4) Атака методом полного перебора

9. Какой алгоритм используется в SSL/TLS для обеспечения конфиденциальности и целостности данных при передаче через интернет?

1) AES
2) RSA
3) DES
4) RC4

10. Какое из этих утверждений о цифровой подписи верно?

1) Цифровая подпись используется для шифрования сообщений
2) Цифровая подпись обеспечивает конфиденциальность сообщения
3) Цифровая подпись используется для проверки подлинности и целостности сообщения
4) Цифровая подпись используется для создания пароля

11. Что такое PKI (Public Key Infrastructure)?

1) Система управления цифровыми подписями
2) Система для шифрования симметричными алгоритмами
3) Система, использующая только одноразовые ключи
4) Механизм для управления и хранения публичных и приватных ключей

12. Что такое "строгий режим шифрования" в контексте алгоритма AES?

1) Режим, где каждый блок данных шифруется отдельно

2) Режим, который запрещает использование всех символов, кроме цифр
3) Режим, использующий блоки фиксированного размера
4) Режим, когда один ключ используется для всех сессий

13. Какой из алгоритмов является алгоритмом хэширования?
1) RSA
2) AES
3) SHA
4) Diffie-Hellman

14. В каком случае используется алгоритм HMAC?
1) Для создания цифровых подписей
2) Для защиты целостности данных
3) Для генерации случайных чисел
4) Для дешифрования сообщений

15. Какой протокол используется для защиты электронной почты с помощью криптографических методов?
1) SSL
2) IMAP
3) S/MIME
4) SMTP

16. Что означает термин "конфиденциальность" в контексте защиты информации?
1) Защита от несанкционированного доступа к данным
2) Удостоверение подлинности отправителя
3) Подтверждение целостности данных
4) Удостоверение авторства данных

17. Какой алгоритм криптографического хэширования используется для проверки подлинности паролей в современных системах?
1) MD5
2) SHA-256
3) DES
4) RSA

18. Что представляет собой метод атакующего, который пытается угадать секретный ключ, исследуя возможные комбинации значений?
1) Атака с радужными таблицами
2) Атака методом полного перебора
3) Атака по словарю
4) Атака с использованием уязвимостей в ПО

19. Что такое "симметричное шифрование"?

1) Использование одинаковых ключей для шифрования и дешифрования
2) Использование двух ключей: публичного и приватного
3) Использование уникальных ключей для каждого сеанса
4) Использование одного ключа для всех пользователей системы

20. Как называется механизм, позволяющий аутентифицировать пользователя с помощью его отпечатка пальца?

1) Биометрическая аутентификация
2) Многофакторная аутентификация
3) Парольная аутентификация
4) Ролевая аутентификация

ПК-3.

21. Какой из перечисленных методов шифрования использует асимметричные ключи?

1) RSA
2) AES
3) DES
4) RC4

22. Для чего используется протокол SSL/TLS?

1) Для шифрования электронных писем
2) Для защиты данных, передаваемых по сети
3) Для аутентификации пользователей
4) Для защиты базы данных

23. Что такое двусторонняя аутентификация (mutual authentication)?

1) Когда только сервер аутентифицирует клиента
2) Когда оба участника обмена информацией аутентифицируют друг друга
3) Когда клиент аутентифицирует себя с помощью пароля
4) Когда оба участника используют одинаковые пароли

24. Какой из методов защиты данных используется для обеспечения целостности и защиты от подмены данных в процессе их передачи?

1) Шифрование
2) Электронная подпись
3) Хэширование
4) Открытые ключи

25. Что такое система управления ключами (KMS)?

1) Механизм для генерации пар ключей
2) Механизм для управления доступом к данным
3) Система для хранения, распределения и защиты ключей
4) Протокол для защиты информации

26. Как называется способ, при котором секретный ключ используется для дешифрования зашифрованных данных?

1) Шифрование с использованием симметричных ключей
2) Асимметричное шифрование
3) Хэширование
4) Электронная подпись

27. Какое из этих утверждений о криптографических хэшах неверно?

1) Хэш-функция всегда генерирует уникальный результат для каждого входа
2) Хэш-функция используется для проверки целостности данных
3) Хэш-функции не могут быть расшифрованы обратно
4) Хэш-функции являются необратимыми

28. Какой из этих алгоритмов шифрования является наиболее эффективным для защиты данных в облачных сервисах?

1) AES
2) RSA
3) Diffie-Hellman
4) ElGamal

29. Какой протокол используется для установления защищенного канала связи между клиентом и сервером в интернете?

1) SSL/TLS
2) HTTP
3) FTP
4) SMTP

30. Как называется метод, при котором два участника обмена могут обмениваться ключами без того, чтобы они были перехвачены третьей стороной?

1) Диффи-Хеллман
2) RSA
3) Эль-Гамаль
4) RSA и Диффи-Хеллман

31. Что такое сертификат X.509?

1) Тип цифровой подписи

2) Стандарт для защиты паролей
3) Формат для хранения и обмена публичными ключами
4) Метод генерации случайных чисел

32. Что представляет собой атака «человек посередине»?

1) Атака, при которой злоумышленник перехватывает и изменяет данные между двумя сторонами
2) Атака на сервер, с целью перегрузить его
3) Атака, при которой пароль пользователя украден с помощью перехвата сети
4) Атака на шифр с использованием радужных таблиц

33. Что такое "многофакторная аутентификация"?

1) Метод, при котором для входа в систему используется два и более разных способа проверки подлинности
2) Использование единого пароля для всех пользователей
3) Использование одноразовых паролей
4) Метод, при котором используется только пароль

34. Что такое криптографическая защита на основе эллиптических кривых?

1) Метод, использующий долгие вычисления для увеличения безопасности
2) Метод, использующий математические особенности эллиптических кривых для обеспечения безопасности
3) Метод, использующий только одноразовые ключи
4) Метод, использующий хэширование

35. Какой из методов защиты данных предполагает использование личных биометрических характеристик, таких как отпечатки пальцев или радужная оболочка глаза?

1) Биометрическая аутентификация
2) Парольная аутентификация
3) Секретный ключ
4) Открытый ключ

36. Какой алгоритм защиты информации используется для цифровых подписей в электронной почте?

1) RSA
2) AES
3) SHA-1
4) DES

37. Какой алгоритм используется в большинстве современных систем для шифрования данных в базе данных?

1) AES
2) RSA
3) MD5
4) SHA-256

38. Какой тип атак чаще всего используется для поиска уязвимостей в криптографических протоколах?

1) Атака «грубой силы»
2) Атака с использованием радужных таблиц
3) Атака на основе шифра
4) Атака по словарю

39. Какой механизм используется для защиты данных в облаке?

1) Симметричное шифрование
2) Асимметричное шифрование
3) Многофакторная аутентификация
4) VPN

40. Как называется процесс, при котором криптографический ключ используется для проверки целостности данных, а не для их шифрования?

1) Хэширование
2) Электронная подпись
3) Аутентификация
4) Диффи-Хеллман

41. Какой алгоритм используется для создания аутентичных цифровых подписей в блокчейне?

1) RSA
2) ECDSA
3) SHA
4) AES

42. Что такое метод "двухфакторной аутентификации"?

1) Использование двух разных криптографических алгоритмов для шифрования
2) Использование комбинации пароля и биометрии для подтверждения личности
3) Использование пароля и одноразового кода, отправленного на телефон
4) Использование двух идентификаторов для каждого пользователя

43. Как называется криптографический протокол, который обеспечивает безопасность веб-сайтов?

1) HTTPS

2) FTP
3) POP3
4) IMAP

44. Какой алгоритм используется в блокчейн-технологиях для проверки транзакций?

1) SHA-256
2) RSA
3) DES
4) MD5

45. Какой тип шифрования используется для передачи конфиденциальных данных в приложениях с использованием публичного ключа?

1) RSA
2) AES
3) SHA
4) DES

Ключ к тесту:

1.2	**2.2**	**3.3**	**4.2**	**5.3**	**6.3**	**7.1**	**8.4**	**9.1**
10.3	**11.4**	**12.1**	**13.3**	**14.2**	**15.3**	**16.1**	**17.2**	**18.2**
19.1	**20.1**	**21.1**	**22.2**	**23.2**	**24.2**	**25.3**	**26.1**	**27.3**
28.1	**29.1**	**30.1**	**31.3**	**32.1**	**33.1**	**34.2**	**35.1**	**36.1**
37.1	**38.1**	**39.1**	**40.2**	**41.2**	**42.3**	**43.1**	**44.1**	**45.1**

Шкала оценивания результатов тестирования

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

6.2.4. Примеры задач при разборе конкретных ситуаций

Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности

ПК-1.

1. Написать отчет о различных источниках угроз безопасности информации, включая внутренние и внешние факторы. Привести примеры атак и их последствия.

2. Разработать политику безопасности для небольшой компании, включая основные элементы, такие как управление доступом, обучение сотрудников и реагирование на инциденты.

3. Оценить риски для информационной системы, используя методику оценки рисков. Определить уязвимости и предложите меры для минимизации рисков.

ПК-3.

4. Провести анализ реальных случаев утечек данных, описывая, как была организована атака и какие меры не были приняты для предотвращения инцидента.

5. Разработать презентацию о стандартах безопасности (например, ISO/IEC 27001), объясняя их значение и применение в организациях.

6. Создать таблицу, в которой будут перечислены различные формы атак на информацию, их описание и способы защиты от них.

Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.

ПК-1.

1. Описать основные криптографические модели, включая симметричные и асимметричные алгоритмы. Привести примеры и объяснить, в каких ситуациях каждую модель следует использовать.

2. Разработать анализ алгоритмов шифрования (например, AES и RSA): принцип работы, преимущества и недостатки каждого алгоритма.

3. Описать методы аутентификации пользователей, включая пароли, токены и биометрию. Привести примеры, где применяются эти методы.

ПК-3.

4. Реализовать простой пример использования алгоритма шифрования (например, AES) на выбранном языке программирования. Описать, как работает код и какие библиотеки использовались.

5. Провести анализ моделей безопасности в одной из операционных систем (например, Windows, Linux). Описать, как они реализуют защиту информации и управление доступом.

6. Исследовать современные угрозы для криптографических методов защиты информации и предложить способы их преодоления.

Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.

ПК-1.

1. Написать отчет о принципах администрирования сетей, включая основные задачи и ответственность сетевого администратора.

2. Описать различные методы защиты информации в сетях, включая фаерволы, системы обнаружения вторжений и VPN. Привести примеры их использования.

3. Разработать концепцию многоуровневой защиты для корпоративной сети, включая физическую, сетевую и прикладную защиту.

ПК-3.

4. Провести практическое исследование по настройке фаервола и системы обнаружения вторжений в тестовой сети. Описать процесс настройки и результаты тестирования.

5. Описать наиболее распространенные угрозах безопасности в сетях и предлагаемые меры по их предотвращению.

6. Разработать руководство по проведению аудита безопасности сетевой инфраструктуры, включая основные этапы и методы.

Тема 4. Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации

ПК-1.

1. Описать основные требования к системам защиты информации, включая функциональные, надежные и устойчивые аспекты.

2. Разработать анализ направлений развития средств безопасности предприятия: новые технологии и подходы.

3. Исследовать правовые аспекты защиты информации: законы и нормативные акты, регулирующие безопасность данных.

ПК-3.

4. Провести исследование о последствиях несанкционированного доступа к информации, приводя примеры из реальной практики.

5. Подготовить отчет о роли регуляторов в обеспечении защиты информации: как они влияют на практики и стандарты безопасности.

6. Описать практические рекомендации по внедрению политики безопасности на уровне предприятия, включая примеры успешных реализаций.

Шкала оценивания

Шкала оценивания	Критерии оценивания
«Отлично»	обучающийся ясно изложил условие задачи, решение обосновал
«Хорошо»	обучающийся ясно изложил условие задачи, но в обосновании решения имеются сомнения;
«Удовлетворительно»	обучающийся изложил решение задачи, но обосновал его формулировками обыденного мышления;
«Неудовлетворительно»	обучающийся не уяснил условие задачи, решение не обосновал либо не сдал работу на проверку (в случае проведения решения задач в письменной форме).

6.2.5. Темы для рефератов

Тема (раздел)	Вопросы
Тема 1. Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК-1 1. Определение криптографии и её роль в защите информации. 2. Основные виды атак на информацию: примеры и способы защиты. 3. Политики безопасности: какие меры необходимо предпринять для защиты информации в организации.

	4. Стандарты безопасности: международные и национальные стандарты по защите информации (например, ISO/IEC 27001). ПК-3 5. Оценка рисков в области информационной безопасности: методы и подходы. 6. Актуальные угрозы безопасности информации в современных информационных системах. 7. Роль человеческого фактора в безопасности информации: как ошибки пользователей могут привести к утечкам данных. 8. Примеры реальных атак на информационные системы и анализ их последствий.
Тема 2. Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	ПК-1 1. Классификация криптографических моделей: симметричные и асимметричные алгоритмы шифрования. 2. Основные алгоритмы шифрования: AES, DES, RSA: принципы работы и области применения. 3. Алгоритмы аутентификации пользователей: методы и средства (например, пароли, токены, биометрия). 4. Модели безопасности в операционных системах: как они реализуют защиту информации. ПК-3 5. Применение криптографических алгоритмов в различных областях: от финансов до государственных структур. 6. Современные угрозы для криптографических методов защиты информации: атаки на шифры и их уязвимости. 7. Интеграция криптографических методов в программное обеспечение и аппаратные решения. 8. Будущее криптографии: новые направления и технологии, такие как квантовая криптография.
Тема 3. Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	ПК-1 1. Основные принципы администрирования сетей: задачи и ответственность сетевого администратора. 2. Методы защиты информации в корпоративных сетях: фаерволы, системы обнаружения вторжений и другие средства. 3. Многоуровневая защита сетевой инфраструктуры: подходы и технологии. 4. Роль VPN и шифрования в защите информации при передаче данных по сетям. ПК-3 5. Примеры успешной реализации многоуровневой защиты в крупных организациях. 6. Угрозы безопасности в сетях: анализ и способы их предотвращения. 7. Аудит безопасности сетевой инфраструктуры: методы и подходы. 8. Практические рекомендации по улучшению безопасности корпоративных сетей.
Тема 4. Требования к системам защиты информации	ПК-1 1. Основные требования к системам защиты информации:

и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	функциональность, надежность, устойчивость. 2. Направления развития средств безопасности: новые технологии и подходы в защите информации. 3. Правовые аспекты защиты информации: законы и нормативные акты, регулирующие безопасность данных. 4. Ответственность организаций за утечку данных: правовые последствия и меры воздействия. ПК-3 5. Примеры несанкционированного доступа к информации и их правовые последствия. 6. Роль регуляторов в обеспечении защиты информации: как они влияют на практики и стандарты безопасности. 7. Разработка и внедрение политики безопасности на уровне предприятия: примеры и рекомендации. 8. Будущее защиты информации: как правовые и технологические изменения повлияют на системы безопасности.

Шкала оценивания

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

6.2.6. Индивидуальные задания для курсовой работы (проекта)

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

6.3. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Вопросы для подготовки к промежуточной аттестации по итогам освоения дисциплины Криптографические методы защиты информации:

ПК-1.

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. Типичные атаки на операционную систему

32. Понятие защищенной операционной системы.

33. Аппаратное обеспечение средств защиты операционной системы.

34. Проблемы безопасности IP-сетей.

35. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP.

36. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой операционной системе (ОС).

37. Назовите элементы безопасности ОС UNIX?

38. Основные практические вопросы зашиты информации.

39. Программные средства защиты и уничтожения информации.

40. Основные принципы построения подсистемы информационной безопасности.

41. Общие принципы обеспечения информационной безопасности.

42. Средства обеспечения конфиденциальности данных.

43. Средства идентификации и аутентификации пользователей.

44. Приведите основные схемы идентификации и аутентификации пользователя.

45. Средства аутентификации электронных данных.

46. Приведите классификацию систем защиты программного обеспечения.

47. Сравните основные технические методы и средства защиты программного обеспечения.

48. Назовите отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования.

49. Приведите определение понятий «протоколирование» и «аудит»

50. Назовите задачи, реализуемые протоколированием и аудитом.

51. Дайте характеристику задачи активного аудита.

52. Принципы построения и свойства потоковых шифров.

53. Основные методы криптоанализа симметричных и асимметричных шифров.

54. Применение криптографических методов для защиты беспроводных сетей.

55. Роль и структура сертификатов открытых ключей (PKI).

56. Механизмы и стандарты цифровой подписи (PKCS, X.509).

57. Алгоритмы генерации ключей и методы управления ключами.

58. Методы обеспечения целостности данных в системах защиты информации.

59. Стандарт ГОСТ Р 34.10-2012 и его применение для электронной подписи.

60. Принципы работы и применение алгоритма RSA.

61. Особенности и применение криптографии с эллиптическими кривыми (ECC).

62. Механизмы анонимности и конфиденциальности в криптографических системах.

63. Основы криптографической защиты мобильных и облачных сервисов.

ПК-3.

64. Современные приложения криптографии. Примеры.

65. Какие элементы безопасности содержит ОС Windows 2000/XP/Vista?

66. Этапы построения подсистемы информационной безопасности.

67. Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными.

68. Правовые последствия несанкционированного съема и использования конфиденциальной информации.

69. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.

70. Перечислите функции и компоненты сети VPN.

71. Классифицируйте VPN по способу технической реализации и архитектуре технического решения.

72. Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

73. Применение асимметричной криптографии в электронной коммерции.

74. Принципы работы и применение протокола SSL/TLS.

75. Особенности построения и использования криптографических токенов.

6.4. 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»

6.4.1. 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	Обучающийся демонстрирует неполное соответствие следующих знаний: Создание инструментальные средства	Обучающийся демонстрирует частичное соответствие следующих знаний: Создание инструментальны	Обучающийся демонстрирует полное соответствие следующих знаний: Создание инструментальны

	средства программирования	программирования	е средства программировани я	е средства программировани я
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять: Разработка 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 утилиты	Обучающийся свободно применяет полученные навыки, в полном объеме владеет навыками работы Разработкой системные утилиты

6.4.2. 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-1. Способен выполнять работы и управление работами по созданию (модификации) и сопровождению ИС, автоматизирую щих задачи организационно го управления и бизнес-процессы	на уровне знаний: знать стандартные задачи профессиональн ой деятельности; знать современные тенденции развития информатики и вычислительной техники, компьютерных технологий и	на уровне умений: уметь применять математически е методы, вычислительну ю технику для решения практических задач; уметь анализировать и выбирать методы и средства	на уровне навыков: элементами функционального анализа; библиотечно-библиографическ ими знаниями.	

	пути их применения в профессиональной деятельности; знать основы информационно-коммуникационных технологий; знать понятия конфиденциальной информации, персональных данных и государственной тайны.	обеспечения информационной безопасности.		
ПК-3. Способен разрабатывать компоненты системных программных продуктов	на уровне знаний: знать сущность и значение информации в развитии в развитии современного информационного общества; знать основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; знать виды угроз, возникающие в процессе информационной деятельности; знать методы и средства обеспечения информационной безопасности объектов профессиональной деятельности.	на уровне умений: уметь выбирать необходимые информационные ресурсы и источники знаний в электронной среде уметь выявлять угрозы информационной безопасности. уметь применять математические методы, вычислительную технику для решения практических задач; уметь анализировать и выбирать методы и средства обеспечения информационной безопасности.	на уровне навыков: 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.	
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.

Промежуточная аттестация обучающихся в форме зачета 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.

7. 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:

- ЭБС «ЛАНЬ» -https://e.lanbook.com/

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

- IPR SMART -https://www.iprbookshop.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.

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

Основная литература:

1. Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561313.

2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52967-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463043. — Режим доступа: для авториз. пользователей.

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/462293. — Режим доступа: для авториз. пользователей.

4. Вавилин, Я. А. Информационные технологии в управлении качеством и защита информации : учебное пособие для вузов / Я. А. Вавилин, В. Г. Солдатов, И. Г. Манкевич. — Санкт-Петербург : Лань, 2025. — 196 с. — ISBN 978-5-507-51437-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/447242. — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915.

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, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560426.

Периодика:

1. Известия Тульского государственного университета. Технические науки: Научный рецензируемый журнал. https://tidings.tsu.tula.ru/tidings/index.php?id=technical&lang=ru&year=1.

- Текст : электронный.

2. Научный периодический журнал «Вестник Южно-Уральского государственного университета. Серия «Вычислительная математика и информатика» : Научный рецензируемый журнал. https://vestnik.susu.ru/cmi - Текст : электронный.

3. Научный периодический журнал «Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника»: Научный рецензируемый журнал. https://vestnik.susu.ru/ctcr - Текст : электронный.

9. 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.
Информационные технологии – периодическое научно-техническое издание в области информационных технологий, автоматизированных систем и использования информатики в различных приложениях novtex.ru	Издательство выпускает теоретические и прикладные научно-технические журналы, обеспечивающие научной, производственной, обзорно-аналитической и образовательной информацией руководящих работников и специалистов промышленных предприятий, научных академических и отраслевых организаций, а также учебных заведений в области приоритетных направлений развития науки и технологий.
Ассоциация инженерного образования России http://www.ac-raee.ru/	Совершенствование образования и инженерной деятельности во всех их проявлениях, относящихся к учебному, научному и технологическому направлениям, включая процессы преподавания, консультирования, исследования, разработки инженерных решений, оказания широкого спектра образовательных услуг, обеспечения связей с общественностью, производством, наукой и интеграции в международное научно-образовательное

	пространство. свободный доступ

10. 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 среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Кабинет систем управления ООО «НПО «Каскад-ГРУП»	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	Yandex браузер	Свободное распространяемое программное обеспечение (бессрочная лицензия)
	МТС Линк	Договор №2/2026 (091_168.ЕП/26) от 27.03.2026
	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)
№ 206б Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Лаборатория «Программирования и баз данных» Лаборатория информационных технологий	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	Windows 7 OLPNLAcdmc Windows Server 2012	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.ЗК/19 от 17.12.19 (бессрочная лицензия)
	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)
	Eclipse IDE for Java EE Developers, NET Framework, JDK 8, Microsoft SQL Server Express Edition, Microsoft Visio Professional, Microsoft Visual Studio, MySQL Installer for Windows, NetBeans, SQL Server Management Studio, Microsoft SQL Server Java Connector, Android Studio, IntelliJ IDEA.	свободно распространяемое программное обеспечение (бессрочная лицензия)

	КОМПАС-3D v20 и v21	Сублицензионный договор № Нп-22-00044 от 21.03.2022 (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 для бизнеса – Расширенный Russian Edition. 150-249 Node 2 year Educational Renewal License	Сублицензионный договор №977_1049.ЕП/25 от 10.12.2025
	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- справочно-правовая система	Договор №С-002-2025 от 09.01.2025
	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)
	МТС Линк	Договор №2/2026 (091_168.ЕП/26) от 27.03.2026
	AIMP	отечественное свободно распространяемое программное обеспечение (бессрочная лицензия)

11. Материально-техническое обеспечение дисциплины

Тип и номер помещения	Перечень основного оборудования и технических средств обучения
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Кабинет систем управления ООО «НПО «Каскад-ГРУП» **№ 219б** (г. Чебоксары, ул. К.Маркса, 60)	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: мультимедийное оборудование (проектор, экран)
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой среднего профессионального образования/бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей) Лаборатория информационных технологий **№ 206б** (г. Чебоксары, ул. К.Маркса, 60)	Оборудование: комплект мебели для учебного процесса; доска учебная; автоматизированные рабочие места, автоматизированное рабочее место преподавателя, проектор и экран; маркерная доска; Технические средства обучения: компьютерная техника (процессор Core i3, оперативная память объемом не менее 8 Гб); сервер в лаборатории (8-ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 1 Тб; мультимедийное оборудование (телевизор)
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

12. Методические указания для обучающегося по освоению дисциплины

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 лабораторного типа.

Выполнению лабораторных работ предшествует проверка знаний студентов – их теоретической готовности к выполнению задания. Проверка

знаний проводится в форме, которую определяет преподаватель дисциплины (тестирование, опрос).

При проведении лабораторных занятий выделяют следующие разделы:

– общие положения (перечень лабораторных или практических
– занятий);
– ообщие требования к выполнению работ;
– инструкция по каждой работе;
– справочные материалы и т. д.

Лабораторные 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.

Готовясь к докладу или выступлению в рамках интерактивной формы, 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.

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

Обучение по данной дисциплине 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 данной дисциплине 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 202__-202__ учебном году на заседании кафедры, протокол № ___ от « » 202 г.

Внесены дополнения и изменения _____
_____
_____
_____
_____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № ___ от « » 202 г.

Внесены дополнения и изменения _____
_____
_____
_____
_____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № ___ от « » 202 г.

Внесены дополнения и изменения _____
_____
_____
_____

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 202__-202__ учебном году на заседании кафедры, протокол № ___ от « » 202 г.

Внесены дополнения и изменения _____
_____
_____
_____
_____