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
«29» марта 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

(наименование дисциплины)

Направление подготовки	**27.03.04 – Управление в технических системах** (код и наименование направления подготовки)
Направленность (профиль) подготовки	**Управление и информатика в технических системах** (наименование профиля подготовки)
Квалификация выпускника	**бакалавр**
Форма обучения	**очная, заочная**

Чебоксары, 2023

Рабочая программа дисциплины разработана в соответствии с:

- федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 27.03.04 Управление в технических системах, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 871 от 31 июля 2020 года, зарегистрированный в Минюсте 26 августа 2020 года, рег. номер 59489 (далее – ФГОС ВО);

- учебным планом (очной формы обучения) по направлению подготовки 27.03.04 Управление в технических системах.

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

Автор Скипина Людмила Николаевна, 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 № 6 от 04.03.2023 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:

– получение студентами знаний о теоретических основах криптографии;

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

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

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

40 Сквозные виды профессиональной деятельности в промышленности (в сферах: обеспечения выпуска (поставки) продукции, соответствующей требованиям нормативных документов и технических условий; метрологического обеспечения разработки, производства, испытаний и эксплуатации продукции; исследования, разработки и эксплуатации средств и систем автоматизации и управления различного назначения; повышения эффективности производства продукции с оптимальными технико-экономическими показателями путем применения средств автоматизации и механизации).

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
40.057 Специалист по автоматизированным системам управления машиностроительным предприятием	B	Ввод в действие АСУП	5	Планирование предварительных испытаний и опытной эксплуатации АСУП	B/02.5	5
			5	Техническое обслуживание АСУП	B/03.5	
	C	Разработка	6	Определение	C/01.6	6
		АСУП		целесообразности автоматизации процессов управления в		

				организации		
		АСУП	6	Разработка информационного обеспечения АСУП	С/02.6	6
			6	Разработка заданий на проектирование оригинальных компонентов АСУП	С/03.6	6
			6	Контроль ввода в действие и эксплуатации АСУП	С/04.6	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**
Разработка АСУП	ПК-2 Разработка информационного обеспечения АСУП	ПК 2.1 Способен проектировать информационную модель данных АСУП, стандартизацию документооборота и характеристик информации	*на уровне знаний*: знать методики поиска, сбора и обработки информации; *на уровне умений:* уметь применять методики поиска, сбора и обработки информации; *на уровне навыков:* владеть практическими навыками поиска и анализа и синтеза информации; ----------
		ПК 2.2 Может разрабатывать технологические схемы обработки информации по отдельным задачам АСУП	*на уровне знаний*: знать актуальные источники информации в сфере профессиональной деятельности; *на уровне умений:* уметь находить и осуществлять систематизацию, критический анализ и синтез информации, полученной из разных источников; *на уровне навыков:*

		ПК 2.3 Способен объединять информационные базы при создании интегрированной АСУП	владеть практическими навыками поиска и обработки информации; ---------- *на уровне знаний*: знать основные принципы и методы системного анализа. *на уровне умений:* уметь применять системный подход для решения поставленных задач направления подготовки. *на уровне навыков:* владеть методикой системного подхода для решения поставленных задач направления подготовки

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.Д(М). В.17 «Криптографические методы защиты информации» является элективной дисциплиной и реализуется в рамках обязательной части Блока 1.

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

Дисциплина «Криптографические методы защиты информации» является промежуточным этапом формирования компетенций ПК-2процессе освоения ОПОП.

Дисциплина «Криптографические методы защиты информации» основывается на знаниях, умениях и навыках, приобретенных при изучении дисциплин: математики, физика, информатика, операционные системы и сети и является предшествующей для изучения дисциплин: учебная практика, производственная практика, государственной итоговой аттестации, выполнении выпускной квалификационной работы.

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

3. Объем дисциплины

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

очная форма обучения:

Семестр	5
лекции	16
лабораторные занятия	16

семинары и практические занятия	-
контроль: контактная работа	-
контроль: самостоятельная работа	-
расчетно-графические работы, курсовые работы (проекты): контактная работа	-
расчетно-графические работы, курсовые работы (проекты): самостоятельная работа	-
консультации	-
Контактная работа	*32*
Самостоятельная работа	*40*

Вид промежуточной аттестации (форма контроля): зачет

заочная форма обучения:

Семестр	6
лекции	4
лабораторные занятия	4
семинары и практические занятия	-
контроль: контактная работа	-
контроль: самостоятельная работа	4
расчетно-графические работы, курсовые работы (проекты): контактная работа	-
расчетно-графические работы, курсовые работы (проекты): самостоятельная работа	-
консультации	-
Контактная работа	*8*
Самостоятельная работа	*60*

Вид промежуточной аттестации (форма контроля): зачет

4. Содержание дисциплины, структурированное по темам (разделам)

Очная форма обучения

Тема (раздел)	Распределение часов			Самостоя-тельная работа	Формируемые компетенции (код)
	Лекции	Лабораторные занятия	Практические занятия		
Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	4	-	4	10	ПК-1, ПК-5
Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	4	-	4	10	ПК-1, ПК-5
Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	4	-	4	10	ПК-1, ПК-5
Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	4	-	4	10	ПК-1, ПК-5

Консультации	-	-	ПК-1, ПК-5
Контроль (зачет)	-	-	ПК-1, ПК-5
ИТОГО	**8**	**40**	

Заочная форма обучения

Тема (раздел)	Распределение часов			Самостоя-тельная работа	Формируемые компетенции (код)
	Лекции	Лабораторные занятия	Практические занятия		
Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	2	-	-	15	ПК-1, ПК-5
Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	2	-	-	15	ПК-1, ПК-5
Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	-	-	2	15	ПК-1, ПК-5
Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	-	-	2	15	ПК-1, ПК-5
Консультации	-			-	ПК-1, ПК-5
Контроль (зачет)	-			4	ПК-1, ПК-5
ИТОГО	**8**			**60**	

5. Образовательные технологии, применяемые при освоении дисциплины

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- Деловая и/или ролевая игра (ДИ);
- Круглый стол, дискуссия, полемика, диспут, дебаты;
- Разноуровневые задачи и задания (РЗЗ) и др.

Под деловой игрой понимается совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально - ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.

Круглый стол, дискуссия, полемика, диспут, дебаты - оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.

Разноуровневые задачи и задания различают:

а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины;

б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно - следственных связей;

в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

6. Практическая подготовка

Практическая подготовка реализуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью. Объем занятий в форме практической подготовки составляет 4 час. (по очной форме обучения), 4 часа (по заочной форме обучения).

Очная форма обучения

Вид занятия	Тема занятия	Количество часов	Форма проведения	Код индикатора достижений компетенции
Практическое задание1	Требования к системам защиты информации и направления развития средств безопасности предприятия.	2	Индивидуальная самостоятельная работа	ПК-2.1 ПК-2.3
Практическое задание 2	Правовые последствия несанкционированного доступа к информации	2	Индивидуальная самостоятельная работа	ПК-2.1 ПК-2.3

Заочная форма обучения

Вид занятия	Тема занятия	Количество часов	Форма проведения	Код индикатора

				достижений компетенции
Практическое задание1	Требования к системам защиты информации и направления развития средств безопасности предприятия.	2	Индивидуальная самостоятельная работа	ПК-2.1 ПК-2.3
Практическое задание 2	Правовые последствия несанкционированного доступа к информации	2	Индивидуальная самостоятельная работа	ПК-2.1 ПК-2.3

7. Учебно-методическое обеспечение самостоятельной работы студентов

Самостоятельная работа студентов предусмотрена учебным планом по дисциплине в объеме 40 часов по очной форме обучения, 60 часа по заочной форме обучения. Самостоятельная работа реализуется в рамках программы освоения дисциплины в следующих формах:

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

В рамках учебного курса предусматриваются встречи с представителями правоохранительных органов.

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

Формы и виды самостоятельной работы студентов: чтение основной и дополнительной литературы – самостоятельное изучение материала по рекомендуемым литературным источникам; работа с библиотечным каталогом, самостоятельный подбор необходимой литературы; работа со словарем, справочником; поиск необходимой информации в сети Интернет; конспектирование источников; реферирование источников; составление аннотаций к прочитанным литературным источникам; составление рецензий и отзывов на прочитанный материал; составление обзора публикаций по теме; составление и разработка терминологического словаря; составление хронологической таблицы; составление библиографии (библиографической

картотеки); подготовка к различным формам текущей и промежуточной аттестации (к тестированию, контрольной работе, зачету); выполнение домашних контрольных работ; самостоятельное выполнение практических заданий репродуктивного типа (ответы на вопросы, задачи, тесты; выполнение творческих заданий).

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

Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит консультирование по выполнению задания, который включает цель задания, его содержания, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. Во время выполнения обучающимися внеаудиторной самостоятельной работы и при необходимости преподаватель может проводить индивидуальные и групповые консультации.

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

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

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

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

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

8.1. Паспорт фонда оценочных средств

№	Контролируемые разделы (темы) дисциплины	Код и наименование компетенции	Индикатор достижения компетенции
1.	Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и стандарты безопасности	ПК 2.1 Способен проектировать информационную модель данных АСУП, стандартизацию документооборота и характеристик информации ПК 2.2 Может разрабатывать технологические схемы обработки информации по отдельным задачам АСУП ПК 2.3 Способен объединять информационные базы при создании интегрированной АСУП	ПК-2.1 Разрабатывает модели бизнес-процессов заказчика ПК-2.2 Выявляет и анализирует требования к ИС ПК-2.3 Разрабатывает архитектуру ИС ПК-2.4 Проектирует ИС ПК-2.3Разрабатывает базы данных ИС ПК-2.1 Владеет технологиями программирования ПК-2.2Владеет технологиями модульного тестирования ИС (верификации) ПК-2.1 Разрабатывает драйверы устройств ПК-2.2 Разрабатывает компиляторы, загрузчики, сборщики ПК-2.3 Разрабатывает системные утилиты
-	Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.		
-	Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.		
4	Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации.		

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 компетенция ПК-2.

Формирования компетенции ПК-2начинается с изучения дисциплины математики, физика, информатика, операционные системы, информационные технологии.

Завершается работа по формированию у студентов указанных компетенций в ходе учебная практика, производственная практика, государственной итоговой аттестации, выполнении выпускной квалификационной работы.

Итоговая оценка сформированности компетенций ПК-2 определяется в подготовке и сдаче государственного экзамена, в выполнении и защите выпускной квалификационной работы.

В процессе изучения дисциплины, компетенции также формируются поэтапно.

Основными этапами формирования ПК-2 при изучении дисциплины «Криптографические методы защиты информации» является последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение студентами необходимыми дескрипторами (составляющими) компетенций. Для оценки уровня сформированности компетенций в процессе изучения дисциплины предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачет.

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

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

Тема (раздел)	Вопросы
Основные понятия и определения. Источники, риски и формы атак на информацию. Политика и	1. Виды информации. Физико-технические особенности проявления информационных процессов.
	2. Конфиденциальность. Целостность. Достоверность. Угроза безопасности. Ущерб безопасности. Уязвимость системы.

стандарты безопасности	3. Атака на компьютерную систему. Комплекс средств защиты. Типичные атаки на компьютерную систему.
	4. Проблемы безопасности IP-сетей. Основные виды сетевых атак.
	5. Доступ. Правила разграничения доступа. Политика безопасности. Групповые политики. Реализация управления доступом. Настройка политики безопасности системы.
	6. Анализ безопасности системы. Понятия и основные положения в информационно-вычислительных системах,
	7. стандарты и спецификации в области информационной безопасности. Технология поддержки электронно-цифровой подписи.
Криптографические модели. Алгоритмы шифрования. Алгоритмы аутентификации пользователей. Модели безопасности основных операционных систем.	1. История криптографии. Основные понятия и определения. Основные системы и стандарты шифрования данных.
	2. Криптографические алгоритмы. Современные приложения.
	3. Понятие о корректирующих кодах. Основные понятия.
	4. Блочный алгоритм шифрования DES.
	5. Режим гаммирования
	6. Алгоритм шифрования RSA.
	7. Хеш-функции MD4 и MD5.
	8. Алгоритм электронной цифровой подписи RSA.
	9. Понятие защищенной ОС. Программное обеспечение защиты ОС.
	10. Модели основных политик безопасности.
	11. Модели и механизмы защиты операционных систем, программного обеспечения.
	12. Протоколирование и аудит.
	13. Средства обеспечения конфиденциальности данных.
	14. Средства идентификации и аутентификации пользователей.
	15. Аутентификация на основе одноразовых многоразовых паролей.
	16. Аутентификация на основе сертификатов.
	17. Биометрические методы аутентификации
Администрирование сетей. Защита информации в сетях. Многоуровневая защита корпоративных сетей.	1. Основные понятия. Топология локальных сетей. Сетевые службы и протоколы.
	2. Администрирование DNS. Установка и администрирование WINS. Управление доменами. Управление пользователями.
	3. Управление компьютерами. Управление сайтами и службами. Управление подсетями.
	4. Уязвимость ОС Windows к сетевым атакам и защита от них. Особенности уязвимости информации обрабатываемой в корпоративных сетях. Цели взлома корпоративных информационных систем. Структура сети.
	5. Информационные потоки. Информационные ресурсы. Разграничение полномочий. Программное и аппаратное обеспечение для функционирования сети.

	6. Источники угроз (антропогенные, техногенные, стихийные). Источники угроз (внутренние и внешние). Последствия реализации угроз. Методы защиты информации (организационные, технические, инженерно-технические, программно-аппаратные). Обобщенные правила противодействия угрозам.
	7. ГОСТ Р ИСО/МЭК 7498-1. Концепция построения защищенных виртуальных сетей VPN. Сетевая модель OSI (базовая эталонная модель взаимодействия открытых систем). Основные принципы построения OSI.
	8. Выбор средств защиты. Сертификат соответствия. Четыре уровня модели подсистемы защиты информации. Средства безопасности сетевых ОС
Требования к системам защиты информации и направления развития средств безопасности предприятия. Правовые последствия несанкционированного доступа к информации	1. Этапы построения подсистемы ИБ. Координированный контроль доступа в нескольких точках. Управление доступом на уровне пользователей. Развитие методов и средств аутентификации. Контроль доступа на основе содержания передаваемой информации. Защита данных при передаче через публичные сети. Интеграция средств контроля доступа и средств VPN. Обнаружение вторжений. Надежность и отказоустойчивость средств защиты. Централизованное управление средствами безопасности.
	2. Ответственность за незаконное получение доступа к информации.

Шкала оценивания ответов на вопросы

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

8.2.2. Темы для докладов

Раздел 1. Корректирующие коды

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

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

Раздел 2. Современные симметричные криптосистемы

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

Раздел 3. Защита в операционных системах

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

Раздел 4. Ассиметричные криптосистемы

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

Шкала оценивания

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

8.2.3. Оценочные средства остаточных знаний (тест)

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

А) Разработка аппаратных средств обеспечения правовых данных

Б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

В) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

А) Хищение жестких дисков, подключение к сети, инсайдерство

Б) Перехват данных, хищение данных, изменение архитектуры системы

В) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

А) Персональная, корпоративная, государственная

Б) Клиентская, серверная, сетевая

В) Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

А) несанкционированного доступа, воздействия в сети

Б) инсайдерства в организации

В) чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

А) Компьютерные сети, базы данных

Б) Информационные системы, психологическое состояние пользователей

В) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

А) Искажение, уменьшение объема, перекодировка информации

Б) Техническое вмешательство, выведение из строя оборудования сети

В) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

А) Экономической эффективности системы безопасности

Б) Многоплатформенной реализации системы

В) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
А) руководители, менеджеры, администраторы компаний
Б) органы права, государства, бизнеса
В) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
А) Установление регламента, аудит системы, выявление рисков
Б) Установка новых офисных приложений, смена хостинг-компании
В) Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
А) Неоправданных ограничений при работе в сети (системе)
Б) Рисков безопасности сети, системы
В) Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
А) Невозможности миновать защитные средства сети (системы)
Б) Усиления основного звена сети, системы
В) Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
А) Усиления защищенности самого незащищенного звена сети (системы)
Б) Перехода в безопасное состояние работы сети, системы
В) Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
А) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Б) Одноуровневой защиты сети, системы
В) Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
А) Компьютерный сбой
Б) Логические закладки («мины»)
В) Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

А) Прочитать приложение, если оно не содержит ничего ценного – удалить
Б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
В) Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
А) Секретность ключа определена секретностью открытого сообщения
Б) Секретность информации определена скоростью передачи данных
В) Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
А) Электронно-цифровой преобразователь
Б) Электронно-цифровая подпись
В) Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
А) Покупка нелицензионного ПО
Б) Ошибки эксплуатации и неумышленного изменения режима работы системы
В) Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
А) Распределенный доступ клиент, отказ оборудования
Б) Моральный износ сети, инсайдерство
В) Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
А) Слабый трафик, информационный обман, вирусы в интернет
Б) Вирусы в сети, логические мины (закладки), информационный перехват
В) Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
А) Потерей данных в системе
Б) Изменением формы информации
В) Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
А) Целостность
Б) Доступность

В) Актуальность

23) Угроза информационной системе (компьютерной сети) – это:
А) Вероятное событие
Б) Детерминированное (всегда определенное) событие
В) Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
А) Регламентированной
Б) Правовой
В) Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
А) Программные, технические, организационные, технологические
Б) Серверные, клиентские, спутниковые, наземные
В) Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
А) Владелец сети
Б) Администратор сети
В) Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
А) Руководств, требований обеспечения необходимого уровня безопасности
Б) Инструкций, алгоритмов поведения пользователя в сети
В) Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
А) Аудит, анализ затрат на проведение защитных мер
Б) Аудит, анализ безопасности
В) Аудит, анализ уязвимостей, риск-ситуаций

29. Что лучше всего описывает цель расчета ALE? Варианты ответа:
а) Количественно оценить уровень безопасности среды
б) Оценить возможные потери для каждой контрмеры
в) Количественно оценить затраты / выгоды
г) Оценить потенциальные потери от угрозы в год

30. Как рассчитать остаточный риск? Варианты ответа:

а) Угрозы х Риски х Ценность актива
б) (Угрозы х Ценность актива х Уязвимости) х Риски
в) SLE х Частоту = ALE
г) (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

1	В	11	А	21	А
2	Б	12	А	22	А
3	А	13	А	23	А
4	А	14	Б	24	В
5	А	15	В	25	А
6	В	16	В	26	А
7	А	17	Б	27	А
8	Б	18	Б	28	В
9	А	19	В	29	Г
10	А	20	Б	30	Г

Шкала оценивания результатов тестирования

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

8.2.4. Темы для самостоятельной работы студентов

Темы для самостоятельной работы:

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

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

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

Типовые темы рефератов

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

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

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

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

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

КР и КП по дисциплине «Зашита информации» рабочей программой и учебным планом не предусмотрены.

8.2.6. ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОГО КОНТРОЛЯ

Вопросы (задания) для зачета:

1. Компьютерные вирусы. Их разновидности.
2. Антивирусные средства. Примеры антивирусных программ.
3. Понятие информационной безопасности.
4. Понятие конфиденциальности информации.
5. Понятие доступа к информации (санкционированный и несанкционированный доступ).
6. Понятия идентификация, аутентификация и авторизация.
7. Понятие угроза безопасности.
8. Понятие уязвимость системы (сети).
9. Понятие атаки на компьютерную систему.
10. Охарактеризуйте подходы к обеспечению компьютерной информации.
11. Перечислите основные и вспомогательные сервисы безопасности, дайте их классификацию.
12. Дайте характеристику групп требований к системе защиты.
13. «Фрагментарный» подход в обеспечении безопасности компьютерной системы.
14. «Комплексный» подход в обеспечении безопасности компьютерной системы.
15. В чем заключается политика безопасности компьютерной системы?
16. На чем основана «избирательная» политика безопасности?
17. На чем основана «полномочная» политика безопасности?
18. Понятие криптографии. Основные виды шифров.
19. Обобщенная схема криптосистемы. Понятия симметричной и асимметричной криптосистемы.
20. Перечислите основные алгоритмы криптографических преобразований.
21. Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях.
22. Как классифицируются средства криптографической защиты информации?
23. Основные достоинства и недостатки алгоритма шифрования данных с помощью DES.
24. Перечислите основные комбинации, используемые при шифровании алгоритмом DES.
25. Перечислите основные режимы работы алгоритма DES.

26. Как обеспечивается криптостойкость асимметричных криптосистем?
27. Каково основное назначение хеш-функции?
28. Каковы основные принципы формирования хеш-функции?
29. Отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хеширования MD5 и SHA.
30. Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия.
31. Современные приложения криптографии. Примеры.
32. Типичные атаки на операционную систему.
33. Понятие защищенной операционной системы.
34. Аппаратное обеспечение средств защиты операционной системы.
35. Проблемы безопасности IP-сетей.
36. Наиболее распространенные варианты атак на компьютерную систему на основе протокола TCP/IP.
37. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой операционной системе (ОС).
38. Какие элементы безопасности содержит ОС Windows 2000/XP/Vista?
39. Назовите элементы безопасности ОС UNIX?
40. Основные практические вопросы зашиты информации.
41. Программные средства защиты и уничтожения информации.
42. Основные принципы построения подсистемы информационной безопасности.
43. Этапы построения подсистемы информационной безопасности.
44. Общие принципы обеспечения информационной безопасности.
45. Средства обеспечения конфиденциальности данных.
46. Средства идентификации и аутентификации пользователей.
47. Приведите основные схемы идентификации и аутентификации пользователя.
48. Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными.
49. Средства аутентификации электронных данных.
50. Правовые последствия несанкционированного съема и использования конфиденциальной информации.
51. Особенности применения технических средств уничтожения информации на магнитных и оптических носителях.
52. Приведите классификацию систем защиты программного обеспечения.
53. Сравните основные технические методы и средства защиты программного обеспечения.
54. Назовите отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования.
55. Приведите определение понятий «протоколирование» и «аудит»
56. Назовите задачи, реализуемые протоколированием и аудитом.

57. Дайте характеристику задачи активного аудита.
58. Перечислите функции и компоненты сети VPN.
59. Классифицируйте VPN по способу технической реализации и архитектуре технического решения.
60. Каковы способы защиты информации при межсетевом взаимодействии?
61. Какие криптографические протоколы используются для защиты технологии «клиент-сервер»?

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

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

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

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

ПК-2 Разработка информационного обеспечения АСУП				
Этап (уровень)	**Критерии оценивания**			
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: - стандартные задачи профессиональной деятельности; - сущность и значение информации в развитии	Обучающийся демонстрирует неполное соответствие следующих знаний: - стандартные задачи профессиональной деятельности; - сущность и значение информации в развитии в развитии современного информационного	Обучающийся демонстрирует частичное соответствие следующих знаний: - стандартные задачи профессиональной деятельности; - сущность и	Обучающийся демонстрирует полное соответствие следующих знаний: - стандартные задачи профессиональной деятельности; - сущность и

	в развитии современного информационного общества; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности; - понятия конфиденциальной информации, персональных данных и государственной тайны.	общества; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности; - понятия конфиденциальной информации, персональных данных и государственной тайны.	значение информации в развитии в развитии современного информационного общества; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности; - понятия конфиденциальной информации, персональных данных и государственной тайны.	значение информации в развитии в развитии современного информационного общества; - современные тенденции развития информатики и вычислительной техники, компьютерных технологий и пути их применения в профессиональной деятельности; - основы информационно-коммуникационных технологий; - основы математики на уровне, необходимом для решения стандартных задач профессиональной деятельности; - виды угроз, возникающие в процессе информационной деятельности; - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности; - понятия конфиденциальной информации, персональных данных и государственной тайны.
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять :	Обучающийся демонстрирует неполное соответствие следующих умений:	Обучающийся демонстрирует частичное соответствие	Обучающийся демонстрирует полное соответствие

	-применять математические методы, вычислительную технику для решения практических задач; - выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности.	-применять математические методы, вычислительную технику для решения практических задач; - выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности.	следующих умений: -применять математические методы, вычислительную технику для решения практических задач; - выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности.	следующих умений: -применять математические методы, вычислительную технику для решения практических задач; - выбирать необходимые информационные ресурсы и источники знаний в электронной среде - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности.
владеть	Обучающийся не владеет или в недостаточной степени владеет : - элементами функционального анализа; - численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; -библиотечно-библиографическими знаниями; - методами и средства обеспечения информационной безопасности.	Обучающийся владеет в неполном объеме и проявляет недостаточность владения навыками : - элементами функционального анализа; - численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; -библиотечно-библиографическими знаниями; - методами и средства обеспечения информационной безопасности.	Обучающимся допускаются незначительные ошибки, неточности, затруднения, частично владеет навыками: -элементами функционального анализа; -численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; -библиотечно-библиографическ	Обучающийся свободно применяет полученные навыки, в полном объеме владеет: -элементами функционального анализа; -численными методами решения систем дифференциальных и алгебраических уравнений, методами аналитической геометрии, теории вероятностей и математической статистики, математической логики, теории графов и теории алгоритмов; -библиотечно-библиографическими знаниями; - методами и

			ими знаниями; - методами и средства обеспечения информационной безопасности.	средства обеспечения информационной безопасности.

8.3.2. Методика оценивания результатов промежуточной аттестации

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

Оценочный лист результатов обучения по дисциплине

Код компетенции	Знания	Умения	Навыки	Уровень сформированности компетенции на данном этапе / оценка
ПК-2 Разработка информационного обеспечения АСУП	Знать: методики поиска, сбора и обработки информации; актуальные источники информации в сфере профессиональной деятельности; основные принципы и методы системного анализа.	Уметь: применять методики поиска, сбора и обработки информации; находить и осуществлять систематизацию, критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач направления подготовки.	Владеть: практическими навыками поиска и анализа и синтеза информации; методикой системного подхода для решения поставленных задач направления подготовки	
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.

9. Электронная информационно-образовательная среда

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронной информационнообразовательной среде Чебоксарского института (филиала) Московского политехнического университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), как на территории филиала, так и вне ее. Электронная информационно-образовательная среда – совокупность информационных и телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ в полном объёме независимо от места нахождения обучающихся Электронная информационно-образовательная среда обеспечивает: а) доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик; б) формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы; в) фиксацию хода образовательного процесса, результатов промежуточной аттестации и

результатов освоения программы бакалавриата; г) проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий; д) взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет». Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации. Основными составляющими ЭИОС филиала являются: а) сайт института в сети Интернет, расположенный по адресу www.polytech21.ru, https://chebpolytech.ru/ который обеспечивает: - доступ обучающихся к учебным планам, рабочим программам дисциплин, практик, к изданиям электронных библиотечных систем, электронным информационным и образовательным ресурсам, указанных в рабочих программах (разделы сайта «Сведения об образовательной организации»); - информирование обучающихся обо всех изменениях учебного процесса (новостная лента сайта, лента анонсов); - взаимодействие между участниками образовательного процесса (подразделы сайта «Задать вопрос директору»); б) официальные электронные адреса подразделений и сотрудников института с Яндекс-доменом @polytech21.ru (список контактных данных подразделений Филиала размещен на официальном сайте Филиала в разделе «Контакты», списки контактных официальных электронных данных преподавателей размещены в подразделах «Кафедры») обеспечивают взаимодействие между участниками образовательного процесса; в) личный кабинет обучающегося (портфолио) (вход в личный кабинет размещен на официальном сайте Филиала в разделе «Студенту» подразделе «Электронная информационно-образовательная среда») включает в себя портфолио студента, электронные ведомости, рейтинг студентов и обеспечивает: - фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися,

- формирование электронного портфолио обучающегося, в том числе с сохранение работ обучающегося, рецензий и оценок на эти работы, г) электронные библиотеки, включающие электронные каталоги, полнотекстовые документы и обеспечивающие доступ к учебно-методическим материалам, выпускным квалификационным работам и т.д.: Чебоксарского института (филиала) - «ИРБИС» д) электронно-библиотечные системы (ЭБС), включающие электронный каталог и полнотекстовые документы: - «ЛАНЬ» - www.e.lanbook.com - Образовательная платформа Юрайт -https://urait.ru е) платформа цифрового образования Политеха -https://lms.mospolytech.ru/ ж) система «Антиплагиат» -https://www.antiplagiat.ru/ з) система электронного документооборота DIRECTUM Standard — обеспечивает документооборот между Филиалом и Университетом; и) система «1С Управление ВУЗом

Электронный деканат» (Московский политехнический университет) обеспечивает фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ обучающимися; к) система «POLYTECH systems» обеспечивает информационное, документальное автоматизированное сопровождение образовательного процесса; л) система «Абитуриент» обеспечивает документальное автоматизированное сопровождение работы приемной комиссии.

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

Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

Дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

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.

11.Профессиональные базы данных и информационно-справочные системы

Профессиональная база данных и информационно-	Информация о праве собственности (реквизиты договора)

справочные системы	
Университетская информационная система РОССИЯ https://uisrussia.msu.ru/	Тематическая электронная библиотека и база для прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права. свободный доступ
научная электронная библиотека Elibrary http://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научно-технических журналов, из которых более 4800 журналов в открытом доступе свободный доступ
сайт Института научной информации по общественным наукам РАН. http://www.inion.ru	Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объём массивов составляет более 3 млн. 500 тыс. записей (данные на 1 января 2012 г.). Ежегодный прирост — около 100 тыс. записей. В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языках, поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифром хранения и ссылками на полные тексты источников из Научной электронной библиотеки.
Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru	Федеральный портал «Российское образование» – уникальный интернет-ресурс в сфере образования и науки. Ежедневно публикует самые актуальные новости, анонсы событий, информационные материалы для широкого круга читателей. Еженедельно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными, репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.

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

Аудитория	Программное обеспечение	Информация о праве собственности (реквизиты договора, номер лицензии и т.д.)
№ **211б** Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и	1С:Предприятие 8. Комплект для обучения	договор № 08/10/2014-0731
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)

техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей). Компьютерный класс. Кабинет информационных систем и технологий ЭЛАРА	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года. Band S: 150-249	Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.ЗК/21 от 24.12.2021 до 31.12.2023
	Google Chrome	Свободное распространяемое программное обеспечение (бессрочная лицензия)
	Microsoft Office Standard 2007(Microsoft DreamSpark Premium Electronic Software Delivery Academic(Microsoft Open License	номер лицензии-42661846 от 30.08.2007) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	Zoom	свободно распространяемое программное обеспечение (бессрочная лицензия)
	AdobeReader	свободно распространяемое программное обеспечение (бессрочная лицензия)
	1С:Предприятие 8. Комплект для обучения	договор № 08/10/2014-0731
№ **207б** Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).Компьютерный класс. Лаборатория моделирования технологических процессов	Kaspersky Endpoint Security Стандартный Educational Renewal 2 года. Band S: 150-249	Номер лицензии 2B1E-211224-064549-2-19382 Сублицензионный договор №821_832.223.ЗК/21 от 24.12.2021 до 31.12.2023
	Windows 7 OLPNLAcdmc	договор №Д03 от 30.05.2012) с допсоглашениями от 29.04.14 и 01.09.16 (бессрочная лицензия)
	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)
	КОМПАС-3D V16 и V17	договор № НП-16-00283 от 1.12.2016 (бессрочная лицензия)
	MathCADv.15	Сублиц.договор №39331/МОС2286 от 6.05.2013) номер лицензии-42661846 от 30.08.2007) (бессрочная лицензия)
	SimInTech	Отечественное программное

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

13. Материально-техническое обеспечение дисциплины

Тип и номер помещения	Перечень основного оборудования и технических средств обучения
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей). Компьютерный класс. Кабинет информационных систем и технологий ЭЛАРА №211б (Чебоксары, ул. К.Маркса, д.60)	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: компьютерная техника; мультимедийное оборудование (проектор, экран)
Учебная аудитория для проведения учебных занятий всех видов, предусмотренных программой бакалавриата/ специалитета/ магистратуры, оснащенная оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин (модулей).Компьютерный класс. Лаборатория моделирования технологических процессов №207б (Чебоксары, ул. К.Маркса, д.60)	Оборудование: комплект мебели для учебного процесса; доска учебная; стенды Технические средства обучения: компьютерная техника
Помещение для самостоятельной работы обучающихся № 112б (г. Чебоксары, ул. К.Маркса. 60)	Оборудование: комплект мебели для учебного процесса; Технические средства обучения: компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Филиала

14. 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 семинарского (практического) типа.

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

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

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

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

Методические указания к самостоятельной работе.

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

Самостоятельная работа в аудиторное время может включать:

1) конспектирование (составление тезисов) лекций;
2) выполнение контрольных работ;
3) решение задач;
4) работу со справочной и методической литературой;
5) работу с нормативными правовыми актами;
6) выступления с докладами, сообщениями на семинарских занятиях;
7) защиту выполненных работ;

8) участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;

9) участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;

10) участие в тестировании и др.

Самостоятельная работа во внеаудиторное время может состоять из:

1) повторения лекционного материала;
2) подготовки к практическим занятиям;
3) изучения учебной и научной литературы;
4) изучения нормативных правовых актов (в т.ч. в электронных базах данных);
5) решения задач, и иных практических заданий
6) подготовки к контрольным работам, тестированию и т.д.;
7) подготовки к практическим занятиям устных докладов (сообщений);
8) подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
9) выполнения курсовых работ, предусмотренных учебным планом;
10) выполнения выпускных квалификационных работ и др.
11) выделения наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на консультациях.
12) проведения самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

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

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

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

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

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

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

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

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ

рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена, обсуждена и одобрена для исполнения в 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 _____
_____
_____
_____
_____