МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»

Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Председатель ПЦК
_____Максаков С. А.
«10» апреля 2026 г.

Рабочая программа дисциплины
ОП.01 Основы информационной безопасности

Закреплена за **ПЦК общепрофессиональных дисциплин; профессиональных модулей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Специальность: **10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность

на базе основного общего образования

Квалификация **техник по защите информации**

Форма обучения **очная**

Общая трудоемкость **84 часов**

Часов по учебному плану 84

в том числе:

контактная работа 80

самостоятельная работа 4

Виды контроля в семестрах:

Зачет с оценкой - 4

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов			
	семестр 4		Итого	
	УП	РП	УП	РП
Лекции	60	60	60	60
Практические	20	20	20	20
Контактная работа	80	80	80	80
Сам. работа	4	4	4	4
Часы на контроль				

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Москва, 2026

Программу составил:
Преподаватель Максаков Сергей Анатольевич _____

Рабочая программа дисциплины
Основы информационной безопасности

Разработана в соответствии с:
Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1553)
06.033. Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)

Разработана на основании учебного плана, утвержденного Учёным советом ФГБОУ ВО "МГУТУ им. К.Г. Разумовского (ПКУ)" от 26.03.2026 протокол №9.

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (УЧЕБНОГО ПРЕДМЕТА)

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ОП

Дисциплина Основы информационной безопасности является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Информатика
2	История
3	Математика
4	Индивидуальный проект (Информатика)
5	Информатика
6	Профильные учебные предметы
Дисциплины (модули) и практики, для которых освоение данной дисциплины необходимо как предшествующее:	
1	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
2	Криптографические средства защиты информации
3	Программные и программно-аппаратные средства защиты информации
4	Учебная практика (защита информации в автоматизированных системах программными и программно-аппаратными средствами)
5	Производственная практика (защита информации в автоматизированных системах программными и программно-аппаратными средствами)
6	Экзамен по модулю (защита информации в автоматизированных системах программными и программно-аппаратными средствами)

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

Цели освоения: 1. Формирование системного понимания ИБ.
2. Усвоение базовых принципов и концепций ИБ.
3. Понимание угроз и уязвимостей.
4. Ознакомление с правовой основой ИБ.
5. Осознание роли человеческого фактора
6. Подготовка базы для дальнейшего обучения (создать прочный фундамент для изучения последующих специальных дисциплин)

Задачи: 1. Изучить основные понятия ИБ.
2. Классифицировать угрозы информационной безопасности.
3. Ознакомиться с основными видами обеспечения ИБ.
4. Изучить нормативно правовое регулирование защиты информации
5. Рассмотреть особенности ИБ в автоматизированных системах (АС).
6. Развить культуру информационной безопасности.

Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 02.3: Знать номенклатуру информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности, в том числе с использованием цифровых средств
ОК 02.4: Уметь определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач
ПК 2.4.: Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.4.1: Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
ПК 2.4.2: Уметь применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
ПК 2.4.3: Иметь практический опыт решения задач защиты от несанкционированного доступа к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ					
Код занятия	**Наименование разделов, тем и содержание занятий /вид занятия/**	**Семестр / Курс**	**Часов/ в том числе**	**Компетен-ции**	**Виды контроля**
	1. Теоретические основы информационной безопасности				
1. 1	Тема 1.1. Основные понятия и задачи информационной безопасности Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности Знать: основные понятия, связанные с информационной безопасностью; примеры преступлений в сфере информации и информационных технологий /Лек/	4	10/0	ПК 2.4.1,ОК 02.3	Устный опрос
1. 2	Практическая работа №1. Основы информационной безопасности: угрозы, риски и методы защиты информации Уметь: выявлять и классифицировать актуальные угрозы ИБ для заданной информационной системы; оценивать величину потенциального ущерба; рассчитывать количественные показатели риска; ранжировать риски по степени критичности и строить матрицу рисков; подбирать адекватные организационные и технические меры защиты для снижения рисков; оформлять результаты анализа в виде формализованной таблицы угроз и рисков. Владеть: понятийным аппаратом ИБ (угроза, уязвимость, атака, риск, остаточный риск); методологией качественного анализа рисков с использованием балльных шкал; навыками работы с табличными процессорами для построения матриц рисков и расчетов; навыками формализации результатов анализа в структурированном табличном виде. /Пр/	4	2/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе
1. 3	Тема 1.2. Основы защиты информации Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности. Знать: понятие целостности, доступности и конфиденциальности; классификацию информации по видам тайны и степени конфиденциальности; цели и задачи защиты	4	8/0	ПК 2.4.1,ОК 02.3	Устный опрос

	информации; модель интеграции информационной безопасности в основную деятельность организации; понятие политики безопасности /Лек/				
1. 4	Практическая работа №2. Проведение инвентаризации и классификации объектов защиты на типовом объекте информатизации (локальная вычислительная сеть офиса организации с выходом в Интернет, серверным оборудованием, автоматизированными рабочими местами пользователей и корпоративными базами данных) Уметь: выявлять и перечислять все элементы информационной системы, подлежащие защите; классифицировать объекты защиты по видам (информация, программное обеспечение, технические средства, персонал, каналы связи); ранжировать объекты защиты по степени критичности для деятельности организации; определять ценность (стоимость) информации для владельца; соотносить каждый объект защиты с возможными угрозами и уязвимостями; составлять реестр (перечень) объектов защиты в формализованном табличном виде Владеть: понятийным аппаратом в области объектов защиты; методикой категорирования информации по степени конфиденциальности и значимости; подходами к определению границ информационной системы; навыками работы с нормативно-правовыми документами в части требований к защите различных видов объектов (152-ФЗ, ФСТЭК России); методами построения реестра активов с присвоением классов защищенности; навыками структурирования и документирования результатов инвентаризации /Пр/	4	4/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе
1. 5	Практическая работа №3. Проведение классификации информационных ресурсов организации по видам охраняемой тайны и степеням конфиденциальности с разработкой перечня сведений, подлежащих защите. Уметь: разграничивать виды информации по категориям доступа ; классифицировать информацию по видам тайны; определять степени конфиденциальности информации и присваивать грифы ограничения доступа; соотносить конкретные информационные ресурсы организации с соответствующими видами тайны и уровнями важности; применять нормативные критерии для отнесения информации к защищаемой; оформлять результаты классификации в виде перечня (описи) сведений, составляющих защищаемую информацию. Владеть: понятийным аппаратом в области режимов защиты информации; нормативной правовой базой в сфере отнесения информации к различным видам тайны; методикой определения степени конфиденциальности информации и установления уровня доступа; критериями отнесения информации к защищаемой; навыками составления перечня сведений, составляющих охраняемую тайну, для конкретной организации; методами документирования результатов классификации в соответствии с установленными требованиями. /Пр/	4	2/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе

1. 6	Тема 1.3. Угрозы безопасности защищаемой информации Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации Знать: понятие угрозы безопасности информации; виды угроз безопасности информации; методы несанкционированного доступа к информации; методы оценки уязвимости информации /Лек/	4	10/0	ПК 2.4.1,ОК 02.3	Устный опрос
1. 7	Практическая работа №4. Проведение идентификации, анализа и классификации угроз информационной безопасности для типового объекта информатизации Уметь: выявлять полный спектр угроз для конкретного объекта информатизации с учетом его архитектуры, режимов работы и среды функционирования; классифицировать угрозы по источникам возникновения; разграничивать угрозы по характеру воздействия; определять нарушаемое свойство информации для каждой угрозы; классифицировать угрозы по способу реализации; оценивать вероятность реализации угрозы с учетом существующих уязвимостей; структурировать выявленные угрозы в формализованном перечне (реестре) с присвоением кодов и категорий. Владеть: понятийным аппаратом в области угроз информационной безопасности; методами идентификации угроз; подходом к построению частной модели угроз для конкретного объекта информатизации в соответствии с требованиями ФСТЭК России; методикой категорирования угроз по степени опасности и вероятности реализации. /Пр/	4	2/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе
	2. Методология защиты информации				
2. 1	Тема 2.1. Методологические подходы к защите информации Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации Знать: факторы, влияющие на уровень защиты; виды мер защиты информации; основные принципы защиты информации /Лек/	4	10/0	ПК 2.4.1,ОК 02.3	Устный опрос
2. 2	Практическая работа №5. Анализ требований нормативных документов, предъявляемых к системе защиты информации типового объекта информатизации, и оценка соответствия применяемых принципов и мер защиты установленным требованиям Уметь: анализировать нормативные и корпоративные требования к защите информации для заданного объекта информатизации; применять базовые принципы информационной безопасности при проектировании системы защиты; соотносить требования и принципы с конкретными угрозами и уязвимостями; оценивать достаточность применяемых мер	4	4/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе

	защиты с точки зрения выполнения установленных требований; выявлять противоречия между требованиями защиты и условиями функционирования объекта; разрабатывать предложения по устранению выявленных несоответствий; оформлять результаты анализа в виде таблицы соответствия требований и реализуемых мер. Владеть: понятийным аппаратом в области методологии защиты информации; основными принципами построения систем защиты информации; нормативной правовой базой, устанавливающей требования к защите информации; методами сравнительного анализа требований и фактического состояния защиты; подходами к оценке эффективности принятых мер защиты; навыками составления актов обследования, ведомостей соответствия, протоколов проверок. /Пр/				
2. 3	Тема 2.2. Нормативно правовое регулирование защиты информации Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации Знать: государственные органы, регулирующие информационную безопасность; ключевые законы РФ в области защиты информации; виды ответственности за преступления в сфере информационной безопасностью; Российские и международные стандарты по защите информации; систему сертификации РФ в области защиты информации /Лек/	4	10/0	ПК 2.4.1,ОК 02.3	Устный опрос
2. 4	Практическая работа №6. Поиск, анализ и систематизация нормативных правовых документов в области защиты информации с использованием справочно-правовой системы Уметь: ориентироваться в интерфейсе справочно-правовых систем («КонсультантПлюс», «Гарант», «Кодекс») для поиска нормативных документов по информационной безопасности; использовать основные инструменты поиска для нахождения актуальных редакций документов; применять гипертекстовые связи между документами для изучения взаимосвязей нормативных актов; использовать функцию «Документы на контроле» для отслеживания изменений в нормативных актах; сохранять и экспортировать найденные документы (фрагменты) в текстовые редакторы для подготовки отчетных материалов; анализировать достоверность и актуальность найденной информации с учетом источников поступления документов. Владеть: понятийным аппаратом в области нормативного обеспечения информационной безопасности; знаниями о структуре и составе основных справочно-правовых систем России, их информационных банков и разделов; методологией поиска нормативных документов с использованием реквизитов; навыками работы с ключевыми понятиями и фильтрами для уточнения поисковых запросов; знаниями о	4	2/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе

	критериях выбора СПС; методами проверки актуальности редакции нормативного документа; навыками составления подборок документов по заданной теме с использованием гипертекстовых связей. /Пр/				
2. 5	Тема 2.3. Защита информации в автоматизированных (информационных) системах Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы Знать: основные механизмы защиты информации; компоненты системы защиты информации; меры защиты в автоматизированных системах; виды программных и программно-аппаратных средств защиты информации; принципы технической охраны объектов информатизации; принципы построения организационно-распорядительной системы /Лек/	4	12/0	ПК 2.4.1,ОК 02.3	Устный опрос
2. 6	Практическая работа №7. Разработка комплекса мер защиты информации для типового автоматизированного рабочего места на основе анализа угроз, требований нормативных документов и категории обрабатываемой информации Уметь: анализировать АРМ на уязвимости; определять угрозы; подбирать меры защиты; обосновывать выбор СЗИ по классу и категории; оценивать достаточность мер; сравнивать варианты по эффективности/стоимости; разрабатывать политику безопасности; оформлять ведомость мер. Владеть: понятиями (АРМ, доверенная загрузка, НСД, антивирус, мониторинг); требованиями ФСТЭК к классам 1Г–3Б и режимам; методами выбора сертифицированных СЗИ; подходами к затратам на защиту; классификацией мер; методами документирования; оценкой экономической эффективности. /Пр/	4	4/0	ПК 2.4.2,ПК 2.4.3,ОК 02.4	Отчет по практической работе
2. 7	Зачет с оценкой ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа /ЗаО/	4	4/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3,ОК 02.3,ОК 02.4	Вопросы к зачёту с оценкой, итоговое тестирование

Список выбранных образовательный технологий:

Название	Описание

Информационные технологии	Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта
Компьютерная технология обучения	Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс не только современным и познавательным, но интересным для обучающихся
Технология поиска информации (Информационная технология)	Информационная технология неотделима от субъектов образовательной деятельности, она является определяющим фактором технологии работы с информацией, применяемой в образовательной практике
Технология организации самостоятельной работы	Организации самостоятельной работы учащихся на более высоком уровне может способствовать применение технологии проектного и проблемного обучения. Методы самостоятельного приобретения знаний основаны на использовании проблемного обучения

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1.1. Основные понятия и задачи информационной безопасности
1. Что именно в информационной сфере понимается под терминами «информация» и «сообщение», и чем эти понятия отличаются друг от друга?
2. Какие конкретные информационные процессы могут выступать в качестве объектов информационной безопасности?
3. Какие виды объектов и систем подлежат защите в рамках обеспечения информационной безопасности?
4. Как в теории информационной безопасности формулируется понятие «угрозы информации»?
5. Что представляет собой «риск информационной безопасности» и из каких компонентов он складывается?
6. Приведите примеры реальных преступлений, совершаемых в сфере информационных технологий, и укажите их состав.
7. В чем заключается сущность и основная цель функционирования системы защиты информации?
8. Каким образом система защиты информации должна обеспечивать защиту человека от опасного контента?
9. Почему неинформированность пользователя в вопросах безопасности рассматривается как одна из ключевых угроз?
10. Какие аспекты деятельности организации охватывает защита человека от опасной информации и от неинформированности?

Тема 1.2. Основы защиты информации
1. Дайте определения трем базовым свойствам информации: целостность, доступность и конфиденциальность.
2. По каким критериям и признакам производится классификация информации по видам тайны и степеням конфиденциальности?
3. В чем принципиальное различие между понятиями «государственная тайна» и «конфиденциальная информация»?
4. Какие этапы включает в себя жизненный цикл конфиденциальной информации в процессе ее создания, обработки и передачи?
5. Какие стратегические цели и тактические задачи ставятся перед системой защиты информации?
6. Какие базовые термины и определения являются основополагающими в области защиты информации (кроме конфиденциальности, целостности и доступности)?
7. Из каких ключевых элементов состоит процесс менеджмента информационной безопасности в организации?
8. Как выглядит модель интеграции информационной безопасности в основную деятельность предприятия?
9. Что представляет собой политика безопасности и какую роль она играет в управлении защитой информации?
10. Как соотносятся между собой цели защиты информации и элементы менеджмента ИБ при построении политики безопасности?

Тема 1.3. Угрозы безопасности защищаемой информации
1. Какое определение дается понятию «угрозы безопасности информации» в нормативных документах?
2. По каким основным признакам строится системная классификация угроз безопасности информации?
3. Какие существуют каналы утечки информации и как они классифицируются?
4. Перечислите основные методы несанкционированного доступа к информации.
5. Что такое «уязвимость» информации и системы защиты, и чем она отличается от угрозы?
6. Какие виды уязвимостей (аппаратные, программные, организационные) наиболее критичны для автоматизированных систем?
7. Назовите основные методы, используемые для оценки уязвимости информации.
8. Как количественно и качественно оценивается уровень уязвимости защищаемой информации?
9. Каким образом каналы несанкционированного доступа соотносятся с конкретными видами угроз?
10. Как знание системной классификации угроз помогает в выборе мер защиты?

Тема 2.1. Методологические подходы к защите информации
1. Какие существующие методики используются для определения требований к защите информации?
2. В чем заключается анализ параметров защищаемой информации при постановке задачи на защиту?
3. Какие внешние и внутренние факторы влияют на требуемый (необходимый) уровень защиты информации?
4. Как производится оценка влияния факторов на итоговый требуемый уровень защищенности?

5. На какие виды делятся меры защиты информации в зависимости от способа реализации?
6. Перечислите и раскройте суть основных принципов защиты информации (например, системность, непрерывность, экономическая целесообразность).
7. В чем заключается различие между превентивными (упреждающими) и реактивными мерами защиты?
8. Как методологические подходы влияют на выбор конкретных средств защиты для разных типов систем?
9. Какие критерии лежат в основе выбора методики для определения требований к защите конкретного объекта?
10. Как принцип «разумной достаточности» реализуется при построении системы защиты?

Тема 2.2. Нормативно правовое регулирование защиты информации
1. Как устроена организационная структура системы защиты информации на уровне государства и на уровне отдельной организации?
2. Какие основные законодательные акты (федеральные законы) составляют правовую базу защиты информации в РФ?
3. Какие российские национальные стандарты (ГОСТы) регламентируют требования к защите информации?
4. С какими международными стандартами (ISO/IEC) гармонизированы российские стандарты в области ИБ?
5. Что представляет собой Система сертификации РФ в области защиты информации и какова ее цель?
6. Какие основные правила установлены в системе сертификации РФ для производителей средств защиты?
7. Какие документы оформляются по итогам сертификации средства защиты информации?
8. Какова роль ФСТЭК России и ФСБ России в нормативном регулировании и сертификации?
9. В чем различие между обязательной и добровольной сертификацией в области защиты информации?
10. Как требования законодательства влияют на разработку локальных нормативных документов организации?

Тема 2.3. Защита информации в автоматизированных (информационных) системах
1. Какие основные механизмы защиты информации реализуются в современных автоматизированных системах?
2. Что входит в состав комплексной системы защиты информации (СЗИ) автоматизированной системы?
3. На какие категории делятся меры защиты, реализуемые в информационных системах (организационные, технические и т.д.)?
4. В чем разница между программными и программно-аппаратными средствами защиты информации?
5. Какие задачи решает инженерная защита и техническая охрана объектов информатизации?
6. Что включает в себя организационно-распорядительная защита информации и каковы ее основные цели?
7. Какие мероприятия по работе с кадрами являются обязательными для обеспечения безопасности информации?
8. Как организуется внутриобъектовый режим и пропускная система на режимных объектах?
9. На каких принципах строится организационно-распорядительная система защиты информации?
10. Как взаимодействуют между собой программно-аппаратные средства и организационно-распорядительные меры для обеспечения целостности и доступности данных?

Задания практических работ представлены в Приложении А.

Оценочные средства промежуточной аттестации:
Вопросы к зачету и ключи правильных ответов см. Приложение А
Темы индивидуальных проектов, курсовых работ (проектов), индивидуальных заданий на практику:
Учебным планом не предусмотрено

Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	ПОРОГОВЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	ПРОДВИНУТЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	ВЫСОКИЙ УРОВЕНЬ Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно» ,«удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

ОК 02.: Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

Недостаточный уровень:
Знает отдельные виды информационных источников (учебник, интернет, инструкция), может назвать 1-2 приёма структурирования (список, заголовок), понимает элементарный формат оформления результатов (текстовый документ, таблица), а также знает названия некоторых устройств (компьютер, принтер, сканер) и программ (Word, Excel).

Умеет под руководством преподавателя формулировать простой запрос (найти дату или определение), использовать один источник (учебник), составлять план поиска из 2 шагов, группировать информацию в список, копировать найденное в текстовый файл.

Пороговый уровень:
Знает номенклатуру основных информационных источников, применяемых в профессиональной деятельности (нормативно-правовые акты, техническая документация, справочные системы, профессиональные сайты, базы данных, ГОСТы, СНиПы, инструкции производителей), основные приёмы структурирования информации (классификация, группировка, ранжирование, выделение главного, составление плана, тезирование), форматы оформления результатов поиска (отчёт, доклад, презентация, таблица, схема, инфографика, аналитическая записка), современные средства и устройства информатизации (ПК, ноутбук, планшет, смартфон, МФУ, сканер, проектор, облачные хранилища), порядок их применения в профессиональной деятельности (включение, настройка, подключение, использование периферии), а также программное обеспечение (операционные системы, офисные пакеты, профессиональные САПР, ГИС, системы документооборота, браузеры, почтовые клиенты).

Умеет самостоятельно определять задачу поиска (цель, ключевые слова), выбирать источники (нормативные документы, справочные системы, сайты), планировать этапы поиска, структурировать информацию в таблицу или план, выделять главное (актуальное, достоверное), оформлять отчёт или презентацию, использовать офисное ПО (Word, Excel, PowerPoint).

Продвинутый уровень:
Знает расширенную номенклатуру информационных источников, включая специализированные (профессиональные форумы, научные базы данных (РИНЦ, Scopus, Web of Science), электронные архивы,

Знает расширенную номенклатуру информационных источников, включая специализированные (профессиональные форумы, научные базы данных (РИНЦ, Scopus, Web of Science), электронные архивы, отраслевые порталы, цифровые библиотеки, реестры (ЕГРН, ЕГРЮЛ), геоинформационные системы, технические каталоги), продвинутые приёмы структурирования информации (дерево целей, матрица, диаграмма Исикавы, интеллект-карты, онтологии, кластеризация), форматы оформления результатов для различных аудиторий (для руководителя — краткая аналитическая записка, для коллег — развёрнутый отчёт, для клиента — презентация с визуализациями), современные устройства информатизации (3D-принтеры, сканеры штрих-кодов, терминалы сбора данных, дроны для мониторинга, носимые устройства), порядок их применения с учётом требований безопасности, а также специализированное программное обеспечение в профессиональной деятельности (САПР AutoCAD/Revit, ГИС QGIS/ArcGIS, бухгалтерские системы 1С, CRM, ERP, системы управления проектами, средства виртуализации).

Умеет декомпозировать сложную задачу на подзадачи для поиска, выбирать источники под контекст (научные базы, реестры, API), планировать поиск с учётом сроков, структурировать информацию в интеллект-карты и диаграммы, оценивать значимость результатов (применимость, эффективность), оформлять результаты для разной аудитории (руководитель, коллеги), использовать профессиональное ПО (САПР, ГИС, 1С, BI-системы).

Высокий уровень:
Знает методологию выбора информационных источников в зависимости от цели и контекста профессиональной задачи (первичные / вторичные, официальные / неофициальные, открытые / закрытые, верифицированные / требующие проверки), методы структурирования неструктурированной и слабоструктурированной информации (контент-анализ, семантический анализ, построение графов знаний), форматы оформления результатов для разных стейкхолдеров с учётом требований к визуализации данных и информационной безопасности, современные и перспективные средства информатизации (IoT-устройства, системы дополненной и виртуальной реальности, биометрические сканеры, квантовые сенсоры), порядок их интеграции в профессиональную деятельность, а также передовое программное обеспечение (системы искусственного интеллекта, нейросети для анализа данных, системы управления базами данных нового поколения, средства автоматизации бизнес-процессов на основе RPA, платформы для работы с большими данными (Hadoop, Spark), BIM-технологии).

Умеет формулировать задачи в условиях неопределённости, проектировать стратегию поиска в распределённых источниках (базы данных, API, реестры), применять продвинутые методы структурирования (графы знаний, онтологии), оценивать практическую значимость с анализом затрат-выгод, создавать мультиформатные результаты (дашборды, интерактивные отчёты), использовать передовые цифровые средства (нейросети, Big Data, цифровые двойники).

ПК 2.4.: Осуществлять обработку, хранение и передачу информации ограниченного доступа

Недостаточный уровень:
Знает отдельные названия СЗИ (антивирус, брандмауэр, пароль), понимает различие между идентификацией и аутентификацией (кто ты / докажи), знает 1-2 криптографических метода (шифрование, хэширование), а также знает, что такое управление доступом (права).

Владеет навыками создания учётной записи и назначения базовых прав по инструкции, генерации ключевой пары ЭП с помощью утилиты под контролем, шифрования файла симметричным ключом (паролем) по образцу, а также проверки целостности файла с помощью хэш-функции по шаблону.

Умеет под руководством преподавателя назначать право на чтение/запись пользователю в БД, выполнять простую проверку прав по инструкции, шифровать строку с помощью онлайн-утилиты, а также подписывать документ ЭП по образцу.

Пороговый уровень:
Владеет навыками решения задач защиты от НСД: настройки разграничения доступа в ОС (DAC/RBAC), настройки антивируса и брандмауэра, шифрования дисков и файлов (BitLocker/LUKS/VeraCrypt), настройки VPN; применения электронной подписи (генерация ключевой пары, подпись, проверка, работа с сертификатами); применения симметричных (AES/ГОСТ, режимы) и асимметричных (RSA/ГОСТ, шифрование, обмен ключами) криптоалгоритмов; использования средств шифрования (СКЗИ: КриптоПро, OpenSSL, GnuPG, шифрование БД, дисков, сетевых соединений); а также документирования выполненных мер защиты.

Умеет самостоятельно применять средства защиты БД (назначение прав доступа на таблицы/строки/столбцы, шифрование столбцов, включение аудита запросов), проверять выполнение требований по защите от НСД при аттестации объектов информатизации (проверка настроек СЗИ в БД, анализ журналов, тестирование на простые атаки (SQL-инъекции)), применять математический аппарат для криптографических преобразований (выполнять арифметические операции в конечных полях, рассчитывать простые числа, хэш-функции), а также использовать типовые программные криптографические средства (СКЗИ: шифрование данных, вычисление хэша; настройка электронной подписи (генерация ключевой пары, подпись, проверка подписи)).

Знает особенности и способы применения программных и программно-аппаратных СЗИ в операционных системах (политики безопасности, контроль учётных записей, аудит, шифрование дисков), компьютерных сетях (межсетевые экраны, VPN, IDS/IPS, сегментация), базах данных (разграничение доступа на уровне таблиц/строк/столбцов, шифрование, аудит запросов); типовые модели управления доступом (дискреционная (DAC), мандатная (MAC), ролевая (RBAC), атрибутная (ABAC)); средства, методы и протоколы идентификации и аутентификации (парольная, двухфакторная, биометрическая, сертификатная; протоколы: PAP, CHAP, Kerberos, RADIUS, TACACS+, OAuth, SAML); основные понятия криптографии (шифрование, дешифрование, ключ, хэш-функция, ЭП, сертификат, PKI); типовые криптографические методы и средства защиты информации

Знает особенности и способы применения программных и программно-аппаратных СЗИ в операционных системах (политики безопасности, контроль учётных записей, аудит, шифрование дисков), компьютерных сетях (межсетевые экраны, VPN, IDS/IPS, сегментация), базах данных (разграничение доступа на уровне таблиц/строк/столбцов, шифрование, аудит запросов); типовые модели управления доступом (дискреционная (DAC), мандатная (MAC), ролевая (RBAC), атрибутная (ABAC)); средства, методы и протоколы идентификации и аутентификации (парольная, двухфакторная, биометрическая, сертификатная; протоколы: PAP, CHAP, Kerberos, RADIUS, TACACS+, OAuth, SAML); основные понятия криптографии (шифрование, дешифрование, ключ, хэш-функция, ЭП, сертификат, PKI); типовые криптографические методы и средства защиты информации (симметричное шифрование (AES, ГОСТ), асимметричное шифрование (RSA, ГОСТ), хэширование (MD5, SHA, ГОСТ), электронная подпись, шифрование дисков, VPN на базе IPsec/OpenVPN, СКЗИ).

Продвинутый уровень:
Умеет самостоятельно настраивать защиту БД для различных СУБД (MS SQL, PostgreSQL, Oracle, MySQL) с учётом требований ФСТЭК, проводить углублённую проверку защищённости при аттестации (пентест БД, анализ уязвимостей), применять математический аппарат для реализации криптографических алгоритмов (AES, RSA, ГОСТ), а также настраивать сертифицированные СКЗИ (КриптоПро, ViPNet) и интегрировать ЭП в приложения.

Знает детальные особенности применения СЗИ для различных классов защищённости, модели управления доступом в специализированных ОС (Astra Linux, SELinux), методы усиления аутентификации (FIDO2, WebAuthn, PKI с аппаратными токенами), криптографические алгоритмы с точки зрения стойкости (длины ключей, режимы шифрования), а также требования нормативных документов (ФСТЭК, ФСБ) к СЗИ, моделям доступа и криптографии.

Владеет навыками проектирования и настройки комплексной защиты от НСД для различных ОС (Astra Linux, Windows, Linux) и классов защищённости (ФСТЭК), применения квалифицированной ЭП в корпоративных системах (интеграция с 1С, ЭДО), выбора и настройки криптоалгоритмов с учётом стойкости (длины ключей, режимы), а также настройки сертифицированных СКЗИ (КриптоПро, ViPNet) для защиты данных на дисках, в БД и в сети.

Высокий уровень:
Умеет самостоятельно проектировать комплексную защиту БД с интеграцией в SIEM и DLP, автоматизировать аттестационные проверки, применять постквантовые криптографические алгоритмы, разрабатывать стратегии использования ЭП в распределённых системах (блокчейн, смарт-контракты), интерпретировать требования регуляторов (ФСТЭК, ФСБ), а также обучать других защите БД, аттестации, криптографии и использованию ЭП.

Знает методологию построения комплексных систем защиты с учётом моделей доступа и криптографии, современные протоколы аутентификации (Zero Trust, непрерывная аутентификация), квантово-стойкие криптографические алгоритмы, постквантовую криптографию, а также стратегии интеграции криптографических методов в гетерогенных и распределённых средах.

Владеет навыками внедрения систем защиты от НСД в гетерогенных и распределённых средах (Zero Trust, микросегментация, EDR), применения постквантовых криптоалгоритмов, интегрирования ЭП с блокчейн и смарт-контрактами, использования гибридной криптографии и квантово-стойких решения, а также обучения других защите от НСД, применению ЭП, симметричных/асимметричных алгоритмов и средств шифрования.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	О.В. Прохорова Информационная безопасность и защита информации:учебник. - СПб.: Лань, 2023. - 124 с.: ил.
Л.1.2	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/336200
Л.1.3	Сидак А. А., Василенко В. В., Рыженко С. В. Информационная безопасность. Физические основы технических каналов утечки информации [Электронный ресурс]:учебное пособие. - Москва: Директ-Медиа, 2022. - 128 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=694670
Л.1.4	Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс]:. - Санкт-Петербург: Лань, 2022. - 44 с. – Режим доступа: https://e.lanbook.com/book/187645
Л.1.5	Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2023. - 131 с. – Режим доступа: https://book.ru/book/949452
Л.1.6	Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий [Электронный ресурс]:Словарь. - Москва: Русайнс, 2024. - 226 с. – Режим доступа: https://book.ru/book/951881
Л.1.7	Мельников В.П., Куприянов А.И., Васильева Т.Ю., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 371 с. – Режим доступа: https://book.ru/book/950148

Л.1.8	Медведев В.А. Информационная безопасность. Введение в специальность + eПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878
Л.1.9	Гилязова Р. Н. Информационная безопасность. Лабораторный практикум [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2026. - 44 с. – Режим доступа: https://e.lanbook.com/book/517536
Л.1.10	Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий [Электронный ресурс]:Словарь. - Москва: Русайнс, 2026. - 226 с. – Режим доступа: https://book.ru/book/959878
Л.1.11	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2026. - 124 с. – Режим доступа: https://e.lanbook.com/book/515187
Л.1.12	Мельников В.П., Куприянов А.И., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2025. - 267 с. – Режим доступа: https://book.ru/book/955528
Л.1.13	Пестунова Т.М., Перов А.А. Информационная безопасность и защита информации: краткое введение и практикум [Электронный ресурс]:Учебное пособие. - Москва: Русайнс, 2025. - 132 с. – Режим доступа: https://book.ru/book/960807

5.1.2. Дополнительная литература

Л.2.1	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2021. - 124 с. – Режим доступа: https://e.lanbook.com/book/158939

5.2. Перечень программного обеспечения

Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition

5.3. Перечень информационных справочных систем

Электронно-библиотечная система "Университетская библиотека онлайн"
Компьютерная справочно-правовая система "КонсультантПлюс"
Сайт национального открытого университета "ИНТУИТ"
Официальный интернет-портал правовой информации
Российский криптографический портал
Российский портал открытого образования

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1302 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочее место преподавателя; маркерная доска; 10 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду;

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1311 - Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; Учебно-наглядные пособия

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические рекомендации по организации самостоятельной работы

СРС – планируемая учебная, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к текущей и промежуточной аттестации. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его

умственных и практических операций и действий зависит и определяется самим студентом.
Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности. На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:
- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.
Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Методические рекомендации по освоению дисциплины (учебного предмета)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.
Работа с рекомендованной литературой:
При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:
- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
- индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
- фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
- решение задач и упражнений по образцу;
- решение вариантных задач и упражнений;
- решение ситуационных производственных (профессиональных) задач;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности.
- выполнение контрольных работ;
- работу с тестами.

При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу;
составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради.
Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;
- оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительными элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова тема и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени

автора. Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата.
Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с
учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь;
работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины.

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по учебной дисциплине (разделу). Тестирование/итоговое тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию/итоговому тестированию студенту необходимо:
- четко выяснить все условия тестирования/итогового тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование/итоговое тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования/итогового тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны
быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки
вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений,

которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

Методические рекомендации по выполнению курсовой работы/ курсового проекта

Курсовая работа/курсовой проект - это учебно-исследовательский труд студента, выполняемый по определённой дисциплине под руководством научного руководителя. Её цель - закрепить и углубить теоретические знания, развить навыки самостоятельного анализа, работы с научной литературой и эмпирическими данными, а также сформировать умения структурировать информацию и формулировать обоснованные выводы.
Курсовая работа/курсовой проект – письменная работа объемом 30–50 страниц, выполняется в несколько этапов:
1. Подготовительный этап
2. Сбор и анализ информации
3. Написание работы
Структура курсовой работы/курсового проекта:
1. Титульный лист – по шаблону вуза.
2. Содержание – разделы с номерами страниц.
3. Введение: актуальность, цель, задачи, объект, предмет, методы, значимость, структура.
4. Основная часть:
o Глава 1 (теоретическая) – анализ концепций, выводы.
o Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
o Глава 3 (рекомендательная, если нужно) – предложения, прогнозы, выводы.
5. Заключение – выводы по задачам, итоги, перспективы.
6. Список литературы – группируйте по типам, оформляйте по ГОСТ, указывайте только использованные источники.
7. Приложения (если нужно) – таблицы, графики, анкеты и т. д. (нумеруются, есть ссылки в тексте).
4. Оформление
5. Проверка и доработка
6. Подготовка к защите
• Доклад (5–7 мин.):
• Презентация.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.
Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.
Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.
Основной формой в дистанционном обучении является индивидуальная форма обучения. Главным достоинством индивидуального обучения для инвалидов и лиц с ограниченными возможностями здоровья является то, что оно позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также обеспечивает возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности.
При изучении дисциплины используются следующие организационные мероприятия:

- использование возможностей сети «Интернет» для обеспечения связи с обучающимися, предоставления им необходимых материалов для самостоятельного изучения, контроля текущей успеваемости и проведения тестирования;

- проведение видеоконференций, лекций, консультаций, и т.д. с использованием программ, обеспечивающих дистанционный контакт с обучающимся в режиме реального времени.
- предоставление электронных учебных пособий, включающих в себя основной материал по дисциплинам, включенным в ОП;

- проведение занятий, консультаций, защит курсовых работ и т.д. на базе консультационных пунктов, обеспечивающих условия для доступа туда лицам с ограниченными возможностями;
- предоставление видеолекций, позволяющих изучать материал курса дистанционно.
- использование программного обеспечения и технических средств, имеющих функции адаптации для использования лицами с ограниченными возможностями.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2026 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2027 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2028 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2029 г. № __
Председатель ПЦК _____

==========

ПРИЛОЖЕНИЕ А

Задания на практические работы

Практическая работа №1

Тема: Основы информационной безопасности: угрозы, риски и методы защиты информации

Задание:

На основе предложенной легенды (описание информационной системы, программного обеспечения, режимов работы сотрудников и существующих уязвимостей) студент должен выполнить следующее:

Составить перечень актуальных угроз для заданного АРМ бухгалтера, классифицируя их по нарушаемому свойству информации (конфиденциальность, целостность, доступность) и источнику возникновения.

Провести качественную оценку рисков для каждой выявленной угрозы с использованием балльной шкалы (вероятность от 1 до 5, ущерб от 1 до 5), рассчитать совокупный уровень риска как произведение вероятности на ущерб и определить категорию каждого риска (низкий, средний, высокий).

Построить графическую матрицу (тепловую карту) рисков в системе координат «Вероятность – Ущерб» с визуальным выделением критической зоны.

Для трех наиболее критичных рисков предложить конкретные организационные и/или технические меры защиты, обосновать их выбор и оценить остаточный уровень риска после внедрения каждой меры.

Сформулировать письменный вывод о самом опасном риске для деятельности компании и перечислить первоочередные мероприятия, подлежащие реализации в первую очередь.

Практическая работа №2

Тема: Проведение инвентаризации и классификации объектов защиты на типовом объекте информатизации (локальная вычислительная сеть офиса организации с выходом в Интернет, серверным оборудованием, автоматизированными рабочими местами пользователей и корпоративными базами данных).

Задание:

На основе предложенной легенды (описание организации, ее структуры, перечня используемого оборудования, программного обеспечения, видов обрабатываемой информации и категорий сотрудников) студент должен выполнить следующее:

Провести инвентаризацию всех элементов информационной системы и составить полный перечень объектов защиты с разделением по следующим категориям: информационные ресурсы (данные), программное обеспечение, технические средства (активное и пассивное сетевое оборудование, серверы, рабочие станции, периферийные устройства), персонал (пользователи и обслуживающий персонал), каналы связи и физическая среда (помещения, системы жизнеобеспечения).

Для каждого выявленного объекта защиты определить его ценность (стоимость) для организации по балльной шкале (например, от 1 до 5) и присвоить категорию значимости (низкая, средняя, высокая, критическая) в зависимости от потенциального ущерба при нарушении свойств информации или выходе объекта из строя.

Определить границы объекта информатизации (зоны ответственности) и выделить основные контуры обработки информации, указав, какие объекты входят в каждый контур.

Для каждого объекта защиты (или групп однородных объектов) сформулировать перечень возможных угроз и уязвимостей, характерных для данного типа объектов, и обосновать необходимость его защиты.

Сформировать итоговый реестр (реестры) объектов защиты в виде структурированной таблицы с обязательными колонками: порядковый номер, наименование объекта, тип объекта, категория значимости, обоснование ценности, предполагаемые угрозы, ответственное лицо (подразделение).

Практическая работа №3

Тема: Проведение классификации информационных ресурсов организации по видам охраняемой тайны и степеням конфиденциальности с разработкой перечня сведений, подлежащих защите.

Задание:

На основе предложенной легенды (описание профиля деятельности организации, перечня обрабатываемых сведений, договорных отношений с контрагентами, кадрового состава, взаимодействия

с государственными органами) студент должен выполнить следующее:

Проанализировать все информационные потоки и ресурсы организации, выделив информацию, которая подлежит отнесению к охраняемым видам тайны (государственная тайна, коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные, налоговая тайна, врачебная тайна и другие в зависимости от легенды).

Для каждой категории охраняемой информации определить:

– нормативно-правовое основание для отнесения к данному виду тайны;

– возможный ущерб при разглашении (по балльной шкале от 1 до 5);

– степень конфиденциальности (например: особой важности, совершенно секретно, секретно, конфиденциально, ДСП – для служебного пользования);

– режим допуска и порядок доступа для сотрудников различных категорий.

Определить, какая информация относится к персональным данным, и установить категорию (общедоступные, специальные, биометрические, иные) в соответствии с 152-ФЗ.

Составить перечень (опись) сведений, составляющих охраняемую тайну организации, в виде структурированной таблицы с обязательными колонками: порядковый номер; наименование сведений (вида информации); вид тайны; степень конфиденциальности (гриф); нормативное основание; предполагаемый ущерб при разглашении (в баллах); категории сотрудников, имеющих доступ.

Разработать предложения по маркировке носителей информации, содержащих сведения различных степеней конфиденциальности, и определить порядок обращения с такими носителями (условия хранения, передачи, уничтожения).

Сформулировать вывод о полноте выявленного перечня защищаемой информации и рекомендации по актуализации перечня (как часто пересматривать, при каких условиях).

Практическая работа №4

Тема: Проведение идентификации, анализа и классификации угроз информационной безопасности для типового объекта информатизации (локальная вычислительная сеть организации с выходом в сеть Интернет, серверным оборудованием, автоматизированными рабочими местами, системой электронного документооборота и базой персональных данных).

Задание:

На основе предложенной легенды (детальное описание объекта информатизации: состав технических средств, используемое программное обеспечение, каналы связи, категории пользователей, режимы обработки информации, физические условия размещения, наличие подключения к внешним сетям) студент должен выполнить следующее:

Провести системный анализ объекта информатизации и выделить все возможные каналы реализации угроз (аппаратные закладки, вредоносное ПО, несанкционированный доступ по сети, физический доступ нарушителя, перехват информации по техническим каналам утечки, социальная инженерия, сбои оборудования и систем жизнеобеспечения).

Составить перечень (реестр) актуальных угроз для заданного объекта информатизации с разделением по следующим классификационным признакам:

– по источнику возникновения (природные, техногенные, умышленные антропогенные, неумышленные антропогенные);

– по характеру воздействия (активные — направленные на модификацию/блокировку, пассивные — направленные на получение информации без изменения системы);

– по нарушаемому свойству информации (конфиденциальность, целостность, доступность);

– по способу реализации (физические, аппаратные, программные, организационно-правовые, психологические);

– по объекту воздействия (информация, программное обеспечение, технические средства, персонал, каналы связи).

Для каждой выявленной угрозы определить возможные уязвимости, которые делают данную угрозу реализуемой (например, для угрозы «Вирусная атака» – уязвимость «Отсутствие антивирусной защиты» или «Несвоевременное обновление баз»).

Проранжировать угрозы по вероятности реализации (от 1 до 5 баллов) с учетом конкретных условий функционирования объекта информатизации (уровень квалификации персонала, наличие средств защиты, физическая охрана объекта и т.д.).

Сформировать итоговый реестр угроз в виде структурированной таблицы с обязательными колонками: порядковый номер; код угрозы (по БДУ ФСТЭК или условное обозначение); наименование угрозы; источники угрозы; объект воздействия; характер воздействия; нарушаемое свойство; способ

реализации; существующие уязвимости; вероятность реализации (балл); возможные последствия.

На основе полученного реестра построить диаграмму распределения угроз по источникам, по нарушаемым свойствам информации и по способам реализации (для наглядного представления структуры угроз).

Сформулировать вывод о наиболее опасных группах угроз для данного объекта информатизации и обосновать необходимость первоочередного принятия защитных мер именно против этих угроз.

Практическая работа №5

Тема: Анализ требований нормативных документов, предъявляемых к системе защиты информации типового объекта информатизации, и оценка соответствия применяемых принципов и мер защиты установленным требованиям.

Задание:

На основе предложенной легенды (описание объекта информатизации, его класса защищенности, уровня значимости персональных данных, наличия сведений, составляющих государственную или коммерческую тайну, а также описание текущего состояния системы защиты информации с перечнем уже внедренных средств и мер) студент должен выполнить следующее:

Провести анализ нормативно-правовой базы, применимой к заданному объекту информатизации, и выделить основные требования к защите информации, включая:

– требования к организационным мерам защиты (назначение ответственных, разработка политик безопасности, инструктажи и обучение, допуск персонала);

– требования к технической защите (средства криптографической защиты, антивирусная защита, межсетевое экранирование, системы обнаружения вторжений, защита каналов связи);

– требования к режиму обработки и хранения информации (маркировка носителей, порядок доступа, учет носителей, порядок уничтожения).

Сформулировать перечень базовых принципов информационной безопасности, которые должны быть реализованы в системе защиты заданного объекта, с обоснованием необходимости каждого принципа (например: принцип минимальных привилегий – для ограничения прав пользователей, принцип эшелонированной защиты – для создания нескольких рубежей обороны, принцип разделения обязанностей – для исключения концентрации полномочий у одного лица).

Провести сравнительный анализ «Требование – Фактическое состояние – Принцип» в виде структурированной таблицы с колонками:

– номер требования;

– нормативный документ и пункт;

– формулировка требования (кратко);

– реализованный принцип ИБ, которому соответствует требование;

– фактическое состояние защиты на объекте (из легенды);

– оценка соответствия (соответствует/не соответствует/частично соответствует);

– выявленные недостатки и риски.

Выявить противоречия между требованиями защиты и текущими условиями функционирования объекта (например, требования к изоляции сегментов сети конфликтуют с необходимостью оперативного обмена данными между отделами; требования к надежности электропитания не выполняются из-за ограниченного бюджета), сформулировать их и предложить варианты разрешения (компромиссные решения).

Разработать перечень рекомендаций по устранению выявленных несоответствий с ранжированием по степени срочности (критические – подлежат устранению немедленно, важные – в ближайшее время, желательные – при плановом развитии системы).

На основе выявленных требований и принципов разработать укрупненную архитектурную схему системы защиты информации для данного объекта, включающую организационный и технический уровни, с указанием основных элементов (система управления доступом, система мониторинга, система антивирусной защиты, система резервного копирования и т.д.).

Сформулировать вывод о полноте и достаточности текущей системы защиты, а также указать, какие принципы ИБ были нарушены (или не реализованы) и к каким рискам это приводит.

Практическая работа №6

Тема: Поиск, анализ и систематизация нормативных правовых документов в области защиты информации с использованием справочно-правовой системы.

Задание:

На основе предложенной тематической задачи (определенный аспект правового регулирования в сфере информационной безопасности: защита персональных данных, требования к государственным информационным системам, лицензирование деятельности по защите конфиденциальной информации, требования к средствам криптографической защиты и др.) студент должен выполнить следующее:

Определить перечень нормативных правовых актов (не менее 5-7 документов), регулирующих заданную область информационной безопасности, используя поисковые возможности справочно-правовой системы (например, карточку поиска в «КонсультантПлюс» или интеллектуальный поиск в «Гарант») . Указать для каждого документа: полное наименование, вид документа, принявший орган, дату принятия и последней редакции, номер.

Изучить структуру найденных нормативных документов и выделить в них ключевые разделы (главы, статьи, пункты), устанавливающие обязательные требования к защите информации для заданного типа объектов (информационные системы персональных данных, государственные информационные системы, объекты критической информационной инфраструктуры и др.).

Для каждого документа определить его место в иерархии нормативных правовых актов (федеральный закон, указ Президента РФ, постановление Правительства РФ, приказ федерального органа исполнительной власти), используя гипертекстовые связи между документами.

Выявить взаимосвязи между найденными документами: какие документы ссылаются на другие, какие утратили силу, какие введены в действие новыми актами (например, в 2025-2026 гг. обновлены требования ФСТЭК России к государственным информационным системам, пересмотрены перечни нормативных актов для лицензионной деятельности).

Составить сводную таблицу «Нормативно-правовое обеспечение заданной области ИБ» с колонками: порядковый номер; вид и наименование документа; принявший орган; дата принятия; действующая редакция (дата); статус документа (действует/утратил силу/частично действует); краткая характеристика регулируемых требований; ссылка на взаимосвязанные документы.

На основе проанализированной нормативной базы сформулировать краткое резюме (10-15 предложений) о составе требований, предъявляемых к защите информации для заданного типа объектов, с выделением наиболее существенных (критических) требований.

Оценить полноту выявленного перечня документов и, при необходимости, дополнить его недостающими актами, используя функцию «Поиск по ситуации» или разделы с комментариями и разъяснениями.

Практическая работа №7

Тема: Разработка комплекса мер защиты информации для типового автоматизированного рабочего места на основе анализа угроз, требований нормативных документов и категории обрабатываемой информации.

Задание:

На основе предложенной легенды (детальное описание АРМ конкретного специалиста: назначение, установленное программное обеспечение, обрабатываемая информация с указанием категории конфиденциальности или вида тайны, наличие сетевого взаимодействия, физические условия эксплуатации, категория пользователя, уровень его квалификации, имеющиеся средства защиты) студент должен выполнить следующее:

1. Провести анализ АРМ как объекта защиты, определив его ключевые характеристики:
   – категория значимости обрабатываемой информации (персональные данные, коммерческая тайна, служебная тайна или иная);
   – класс защищенности АРМ (с использованием приказа ФСТЭК России от 18.02.2013 № 21 или методики определения класса) ;
   – критичные элементы, подлежащие первоочередной защите;
   – существующие уязвимости (из легенды или выявленные самостоятельно).
2. На основе проведенного анализа сформулировать перечень актуальных угроз для данного АРМ (по аналогии с практической работой №4) и для каждой угрозы оценить уровень риска (вероятность × ущерб).
3. Для каждой выявленной угрозы (или группы однородных угроз) подобрать конкретные меры защиты в соответствии с классификацией:
   – Организационные меры: назначение ответственных лиц за эксплуатацию АРМ, разработка инструкции пользователя, ограничение физического доступа к АРМ, организация обучения и инструктажей, регламент резервного копирования, порядок реагирования на инциденты.
   – Технические меры: средства антивирусной защиты (с указанием конкретного ПО из реестра

ФСТЭК), средства защиты от несанкционированного доступа (СЗИ от НСД — например, «Соболь», «Аккорд-АМДЗ», «ПАК "МАК"»), межсетевое экранирование (персональный межсетевой экран), система обнаружения вторжений, средства криптографической защиты (СКЗИ) при необходимости шифрования дисков или электронной подписи, система резервного копирования (встроенные средства ОС или специализированное ПО), защита каналов связи (VPN) при удаленной работе, биометрические средства аутентификации.

– Физические меры: установка АРМ в охраняемом помещении с ограничением доступа, использование замков на системный блок, опломбирование портов и разъемов.

4. Для выбранных мер защиты заполнить ведомость в виде таблицы с колонками:

– порядковый номер;

– выявленная угроза (или группа угроз);

– рекомендуемая мера защиты (организационная/техническая/физическая);

– конкретное наименование СЗИ (для технических мер) или описание действия (для организационных);

– документ, устанавливающий требование к мере (нормативный акт);

– оценка остаточного риска после внедрения меры (в баллах по шкале 1-5);

– примечание (стоимость, сложность внедрения, приоритет).

5. Обосновать выбор конкретного типа СЗИ для технических мер с учетом класса защищенности АРМ и требований ФСТЭК (например, для АРМ класса 1Г обязательно использование СЗИ от НСД с функцией очистки остаточной информации и доверенной загрузки). Указать возможные альтернативные варианты и обосновать, почему выбран именно предложенный вариант (критерии: сертификация, стоимость, совместимость, простота администрирования).

6. Разработать инструкцию пользователя АРМ в части правил работы и ограничений (краткая памятка на 1-2 страницы), включающую:

– правила авторизации (использование сложных паролей, периодичность смены, блокировка при уходе);

– запрет на установку неразрешенного ПО;

– правила работы с внешними носителями информации;

– обязанность по регулярному резервному копированию;

– порядок действий при обнаружении признаков вирусной атаки или нарушения доступа;

– запрет на передачу паролей и ключей третьим лицам.

7. Оценить стоимостные затраты на реализацию предложенного комплекса мер (условно, в стоимостных единицах или по шкале «низкие/средние/высокие»), сопоставить их с прогнозируемым ущербом от реализации угроз, сделать вывод об экономической целесообразности предлагаемых мер.

8. Сформулировать итоговый вывод о составе и достаточности выбранных мер защиты для данного АРМ, указав, какие риски снижаются до приемлемого уровня, а какие остаются (остаточные риски) и требуют дополнительного контроля или страхования.

ПРИЛОЖЕНИЕ Б

Вопросы к зачёту с оценкой

Индикатор ЗНАТЬ:

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

1. Установите правильную последовательность этапов жизненного цикла конфиденциальной информации в процессе ее обработки в организации

А) Передача информации адресату или в архив

Б) Создание или получение документа (носителя)

В) Уничтожение или передача в архив после истечения срока хранения

Г) Обработка и использование информации в соответствии с целями

2. Установите правильную последовательность действий при реализации угрозы несанкционированного доступа к информации в автоматизированной системе

А) Преодоление систем защиты (средств разграничения доступа)

Б) Сбор информации об объекте (разведка)

В) Получение несанкционированного доступа к ресурсам системы

Г) Реализация вредоносных действий (модификация, копирование, блокировка)

3. Установите правильную последовательность этапов построения системы защиты информации в организации

А) Внедрение выбранных организационных и технических мер защиты

Б) Проведение анализа рисков и оценки уязвимостей

В) Определение перечня защищаемой информации и требований к ее защите

Г) Разработка политики безопасности и организационно-распорядительных документов

4. Установите правильную последовательность мер защиты информации по степени их приоритетности при организации внутриобъектового режима

А) Оснащение помещений техническими средствами охраны и контроля доступа

Б) Организация пропускного режима и контроля перемещения сотрудников и посетителей

В) Определение перечня режимных помещений и зон с ограниченным доступом

Г) Назначение ответственных лиц за обеспечение внутриобъектового режима

5. Установите соответствие между базовым свойством информации и его содержательной характеристикой

А) Конфиденциальность

Б) Целостность

В) Доступность

Г) Аутентичность (подлинность)

1. Свойство информации быть своевременно полученной уполномоченным пользователем
2. Свойство информации не быть измененной или уничтоженной несанкционированно
3. Свойство информации быть доступной только субъектам, имеющим на то право
4. Свойство информации, гарантирующее, что она исходит от заявленного источника
5. Свойство информации быть понятной для всех категорий пользователей без ограничений

6. Установите соответствие между видом угрозы безопасности информации и ее характеристикой

А) Угроза перехвата информации

Б) Угроза модификации информации

В) Угроза уничтожения информации

Г) Угроза блокировки информации

1. Несанкционированное изменение содержания данных, нарушающее их достоверность
2. Получение доступа к содержимому информации без нарушения ее логической структуры
3. Сделать информацию недоступной для легитимных пользователей без ее удаления
4. Полное физическое или логическое удаление данных с носителя
5. Нарушение целостности программного обеспечения, приводящее к сбоям

7. Установите соответствие между категорией мер защиты информации и конкретным примером такой меры

А) Организационно-распорядительная мера

Б) Программно-аппаратная мера

В) Инженерно-техническая мера

Г) Правовая мера

1. Установка системы шифрования данных на серверах организации
2. Заключение трудового договора с условиями о неразглашении коммерческой тайны
3. Внедрение системы видеонаблюдения и охранной сигнализации по периметру объекта
4. Издание приказа о назначении ответственного за защиту информации
5. Проведение обучения сотрудников правилам безопасной работы в интернете

8. Установите соответствие между этапом жизненного цикла конфиденциальной информации и действием, выполняемым на этом этапе

А) Этап создания документа

Б) Этап обработки и использования

В) Этап хранения

Г) Этап уничтожения

1. Выполнение регламентных операций с данными в соответствии с должностными обязанностями
2. Обеспечение физической сохранности носителя в сейфе или специальном помещении
3. Принятие решения о необходимости дальнейшего хранения или окончательной ликвидации
4. Подготовка акта об уничтожении и приведение носителя в состояние, исключающее восстановление
5. Разработка и утверждение формы документа или структуры базы данных

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

9. Установите правильную последовательность этапов сертификации средства защиты информации в Российской Федерации

А) Проведение сертификационных испытаний и оформление протоколов

Б) Подача заявки в уполномоченный орган по сертификации

В) Выдача сертификата соответствия и внесение в реестр

Г) Анализ заявки и технической документации на средство защиты

10. Установите правильную последовательность мероприятий по работе с кадрами в целях обеспечения информационной безопасности

А) Проведение периодических инструктажей и проверок знаний требований безопасности

Б) Ознакомление сотрудника под подпись с политикой безопасности и должностными инструкциями

В) Проверка благонадежности сотрудника при приеме на работу

Г) Прекращение доступа и сдача носителей информации при увольнении

11. Установите правильную последовательность действий при внедрении программно-аппаратных средств защиты в информационную систему

А) Тестирование работоспособности средств защиты в штатном режиме

Б) Установка и настройка программно-аппаратных модулей на защищаемые узлы

В) Анализ архитектуры системы и выбор конкретных средств защиты

Г) Ввод в промышленную эксплуатацию и мониторинг эффективности защиты

12. Установите соответствие между субъектом системы сертификации РФ в области защиты информации и его функцией

А) Федеральная служба по техническому и экспортному контролю (ФСТЭК)

Б) Федеральная служба безопасности (ФСБ)

В) Орган по сертификации

Г) Испытательная лаборатория

1. Проведение сертификационных испытаний средств защиты информации и оформление протоколов
2. Установление требований к защите информации, не содержащей государственную тайну
3. Рассмотрение заявок и выдача сертификатов соответствия на средства защиты
4. Координация деятельности в области криптографической защиты информации
5. Осуществление обязательного страхования ответственности обладателей информации

13. Установите соответствие между элементом политики безопасности организации и его содержанием

А) Цель политики безопасности

Б) Объект защиты

В) Субъект доступа

Г) Ответственность за нарушение

1. Конкретный пользователь, процесс или устройство, запрашивающее доступ к ресурсам
2. Определение мер дисциплинарной, административной и уголовной ответственности
3. Обеспечение непрерывности бизнес-процессов при сохранении трех базовых свойств информации
4. Информационные ресурсы, программное обеспечение и технические средства
5. Правила резервного копирования и восстановления данных в случае аварии

14. Установите соответствие между методом несанкционированного доступа к информации и его кратким описанием

А) Непосредственный доступ (физический)

Б) Электромагнитный перехват (побочные излучения)

В) Социальная инженерия

Г) Программная закладка

1. Получение доступа к компьютеру или носителю в отсутствие владельца с использованием его учетных данных
2. Психологическое воздействие на персонал с целью получения паролей или конфиденциальных сведений
3. Специально внедренный вредоносный код, позволяющий удаленно управлять системой
4. Перехват сигналов, излучаемых монитором, принтером или сетевым оборудованием
5. Использование уязвимостей в протоколах маршрутизации для перенаправления трафика

15. Установите соответствие между принципом построения организационно-распорядительной системы защиты и его смысловым наполнением

А) Принцип персональной ответственности

Б) Принцип непрерывности защиты

В) Принцип минимальной привилегии

Г) Принцип системности

1. Предоставление сотруднику только тех прав доступа, которые необходимы для выполнения его прямых обязанностей
2. Увязка всех мер защиты (организационных, технических, правовых) в единый комплекс
3. Закрепление конкретных зон ответственности за каждым руководителем и специалистом
4. Осуществление защитных мероприятий постоянно, на всех этапах обработки информации
5. Обязательное дублирование всех критичных систем защиты для повышения надежности

Индикатор УМЕТЬ:

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

1. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор

Что из перечисленного является ключевым отличием понятия «риск информационной безопасности» от понятия «угроза информационной безопасности»?

А) Риск всегда реализуется только в результате преднамеренных действий злоумышленника

Б) Риск представляет собой потенциальную возможность нарушения свойств информации, а угроза – уже свершившееся событие

В) Риск учитывает вероятность реализации угрозы и величину возможного ущерба, тогда как угроза лишь констатирует саму возможность воздействия

Г) Риск относится только к конфиденциальной информации, а угроза – ко всей информации без исключения

2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор

В каком из перечисленных случаев нарушается свойство целостности информации, а не ее доступности или конфиденциальности?

А) Сервер организации перестал отвечать на запросы из-за DDoS-атаки

Б) Сотрудник случайно скопировал базу клиентов на личную флеш-карту

В) В результате сбоя программного обеспечения все суммы в платежных документах увеличились на десять процентов

Г) Пароль учетной записи был перехвачен при передаче по незащищенному каналу связи

3. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор

Какая последовательность действий в наибольшей степени соответствует логике интеграции информационной безопасности в основную деятельность организации?

А) Разработка политики безопасности → внедрение средств защиты → определение угроз → анализ рисков

Б) Определение угроз → разработка политики безопасности → внедрение средств защиты → анализ рисков

В) Анализ рисков → определение угроз → разработка политики безопасности → внедрение средств защиты

Г) Определение защищаемых активов → анализ рисков → разработка требований → внедрение мер защиты

4. Прочитайте текст и запишите развернутый ответ. В коммерческом банке внедрена многоуровневая система защиты информации: установлены межсетевые экраны, используется двухфакторная аутентификация, применяется шифрование каналов связи, а доступ сотрудников к базам данных строго разграничен по ролям. Однако в ходе внутреннего аудита выяснилось, что около 40% сотрудников используют простые пароли, записывают их на стикеры и приклеивают к мониторам, а также что в организации отсутствует регулярное обучение персонала правилам информационной безопасности. В результате этого системный администратор стал жертвой фишинговой атаки и предоставил злоумышленникам удаленный доступ к серверу резервного копирования. Оцените, какое из трех базовых свойств информации (конфиденциальность, целостность, доступность) было нарушено в первую очередь в описанной ситуации, и почему все перечисленные программно-аппаратные средства не смогли предотвратить инцидент.

5. Прочитайте текст и запишите развернутый ответ. В организации, имеющей лицензию на работу со сведениями, составляющими государственную тайну, был разработан новый программный продукт, который должен обрабатывать секретные данные в автоматизированной системе. Руководство приняло решение не проводить обязательную сертификацию этого программного продукта и системы в целом, ссылаясь на то, что продукт разработан собственными силами, а все разработчики имеют допуск к государственной тайне. Также было решено не устанавливать сертифицированные средства криптографической защиты, а использовать собственные алгоритмы шифрования, разработанные внутренним отделом. Оцените правомерность таких решений с точки зрения российского законодательства в области защиты информации и системы сертификации. Какие нормативные акты и органы регулируют данную сферу, и каковы возможные последствия для организации при проверке регулирующими органами?

6. Прочитайте текст и запишите ответ. В организации обрабатывается 800 документов, содержащих конфиденциальную информацию. Согласно политике безопасности, доступ к документам имеют только сотрудники, прошедшие специальную проверку. В штате организации 200 сотрудников. Из них допуск к конфиденциальной информации имеют 120 человек, а остальные работают только с открытыми данными. В ходе проверки выяснилось, что 15% сотрудников, имеющих доступ, нарушают правила хранения документов (оставляют на рабочих столах), а 25% сотрудников, не имеющих доступа, пытались получить его несанкционированно (по данным системы мониторинга). Сколько сотрудников, имеющих доступ, нарушают правила хранения документов? Разрешается использовать калькулятор. В ответе укажите только число.

7. Прочитайте текст и запишите ответ. Для защиты информации в автоматизированной системе используются три уровня парольной защиты. Вероятность взлома одного уровня защиты составляет 0,1 (10%). Для получения полного доступа злоумышленник должен последовательно преодолеть все три уровня, причем каждый следующий уровень взламывается независимо от предыдущего. Сколько процентов составляет вероятность успешного преодоления всех трех уровней защиты (ответ запишите целым числом без знака процента)? Разрешается использовать калькулятор. В ответе укажите только число.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

8. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор

Какая мера относится к организационно-распорядительным методам защиты информации, а не к инженерно-техническим или программным?

А) Установка межсетевого экрана для фильтрации трафика между сегментами сети

Б) Разработка и утверждение перечня должностей, имеющих доступ к коммерческой тайне

В) Монтаж системы контроля доступа с использованием биометрических считывателей

Г) Шифрование содержимого жестких дисков на всех персональных компьютерах организации

9. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор

Согласно российскому законодательству и системе сертификации, какое из перечисленных средств защиты информации обязательно подлежит сертификации на соответствие требованиям безопасности?

А) Любое антивирусное программное обеспечение, распространяемое на территории РФ

Б) Средства криптографической защиты информации, используемые в государственных информационных системах

В) Все программные продукты, обрабатывающие персональные данные граждан РФ

Г) Средства резервного копирования и восстановления данных любого производителя

10. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При построении системы защиты информации в автоматизированной системе нарушение какого принципа организационно-распорядительной защиты делает бессмысленным применение самых совершенных программно-аппаратных средств?

А) Принципа непрерывности защиты во времени

Б) Принципа персональной ответственности за сохранность информации

В) Принципа экономической целесообразности затрат на защиту

Г) Принципа минимальной привилегии для пользователей

11. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. В контексте управления уязвимостями, какое утверждение наиболее точно характеризует различие между уязвимостью и угрозой?

А) Уязвимость – это слабость системы, которая может быть использована для реализации угрозы, в то время как угроза – это сам процесс использования этой слабости

Б) Уязвимость всегда является следствием ошибок разработчиков программного обеспечения, а угроза всегда связана с действиями человека

В) Уязвимость относится только к техническим средствам защиты, а угроза – только к организационным мерам

Г) Уязвимость и угроза являются тождественными понятиями и используются как синонимы в нормативных документах

12. Прочитайте текст и запишите развернутый ответ. На крупном промышленном предприятии произошел инцидент: в результате скачка напряжения в электрической сети вышел из строя контроллер, управляющий технологическим процессом. Аварийная защита сработала некорректно, и давление в трубопроводе превысило допустимые значения, что привело к выбросу вредных веществ. Расследование показало, что система мониторинга давления своевременно фиксировала превышение, но сигнал тревоги не был отправлен на пульт оператора из-за сбоя в программном обеспечении, которое давно не обновлялось. При этом резервный канал связи также оказался неработоспособным, так как его техническое обслуживание не проводилось в течение полугода. Проанализируйте, какие виды угроз (естественные, техногенные, преднамеренные) имели место в данной ситуации, какие из них были первичными, а какие – вторичными. Также определите, какие принципы организационно-распорядительной защиты информации были нарушены, и какие меры следовало бы предусмотреть для предотвращения подобных инцидентов с точки зрения обеспечения доступности информации.

13. Прочитайте текст и запишите развернутый ответ. В ходе планового аудита информационной безопасности в государственном учреждении было установлено, что все рабочие станции подключены к единой локальной сети без сегментации, сотрудники используют одинаковые локальные учетные записи с правами администратора, а удаленный доступ к серверам осуществляется через незащищенный протокол без использования VPN. При этом внутри здания отсутствует система контроля доступа в серверную комнату, дверь в которую часто остается открытой. Финансирование на модернизацию системы защиты выделено, но его освоение запланировано только на следующий год. В то же время учреждение обрабатывает персональные данные граждан и сведения ограниченного доступа. Опишите, какие каналы несанкционированного доступа к информации существуют в описанной ситуации, и классифицируйте их по способу реализации (физические, технические, организационные, программные).

На основе модели интеграции информационной безопасности в деятельность организации предложите приоритетный план неотложных мероприятий, которые можно реализовать без значительных финансовых затрат в кратчайшие сроки.

14. Прочитайте текст и запишите ответ. На предприятии установлено 4 системы видеонаблюдения, 3 системы контроля доступа и 2 системы охранной сигнализации. В течение года произошло 12 инцидентов, связанных с нарушением физической защиты периметра. При этом системы видеонаблюдения зафиксировали 8 инцидентов, системы контроля доступа предотвратили 4 попытки проникновения, а системы охранной сигнализации сработали 6 раз (некоторые инциденты фиксировались несколькими системами одновременно). Эффективность системы видеонаблюдения определяется как отношение числа зафиксированных инцидентов к общему числу систем видеонаблюдения. Чему равна эффективность одной системы видеонаблюдения (ответ запишите целым числом)? Разрешается использовать калькулятор.

15. Прочитайте текст и запишите ответ. В автоматизированной системе обрабатывается 500 документов. Из них 40% содержат персональные данные, 30% – коммерческую тайну, а остальные – общедоступную информацию. Система защиты информации должна обеспечивать разные уровни доступа: к персональным данным – 50 сотрудников, к коммерческой тайне – 30 сотрудников, к общедоступной информации – все 120 сотрудников организации. При этом один сотрудник может иметь доступ к нескольким категориям информации одновременно. Всего в организации 120 сотрудников, каждый из которых имеет доступ хотя бы к одной категории. Сколько сотрудников имеют доступ одновременно и к персональным данным, и к коммерческой тайне, если известно, что количество сотрудников, имеющих доступ только к общедоступной информации, равно 50? Разрешается использовать калькулятор.

Индикатор ИМЕТЬ НАВЫКИ И (ИЛИ) ОПЫТ ДЕЯТЕЛЬНОСТИ:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Прочитайте текст и запишите ответ (только целое число). В организации действует система грифов секретности. Документы распределены по трем уровням: "Особой важности" – 25 документов, "Секретно" – 45 документов, "Для служебного пользования" – 80 документов. Каждый документ должен храниться в отдельном сейфе. В наличии имеются сейфы трех типов: тип А вмещает 5 документов любого грифа, тип Б – 10 документов, тип В – 20 документов. Руководство решило закупить минимальное количество сейфов так, чтобы документы каждого грифа хранились отдельно от других грифов (в разных сейфах), но при этом все сейфы одного типа. Сколько всего сейфов типа В необходимо закупить, чтобы разместить все документы?

2. Прочитайте текст и запишите ответ (только целое число).Система резервного копирования данных имеет следующую эффективность: полное копирование всех данных занимает 4 часа, инкрементальное (только измененные данные) – 1 час, дифференциальное (изменения с момента последнего полного) – 2 часа. Полное копирование выполняется каждое воскресенье, инкрементальное – каждый рабочий день (понедельник-пятница), дифференциальное – по субботам. За неделю объем изменяемых данных в среднем составляет 20% от общего объема. Сколько всего часов в неделю занимает резервное копирование по данному графику?

3. Прочитайте текст и запишите ответ (только целое число). В системе защиты информации используется ролевая модель доступа. Имеются 4 роли: "Администратор", "Менеджер", "Оператор", "Гость". Права доступа распределены так: Администратор имеет доступ ко всем 100 документам, Менеджер – к 70 документам, Оператор – к 40 документам, Гость – к 10 документам. Известно, что документы, доступные Гостю, полностью входят в набор документов Оператора. Документы Оператора полностью входят в набор Менеджера. Документы Менеджера полностью входят в набор Администратора. Сколько документов доступно ровно трем ролям из четырех?

4. Прочитайте текст и запишите ответ (только целое число). Политика безопасности организации требует, чтобы пароль сотрудника содержал не менее 8 символов, включал хотя бы одну цифру и одну заглавную букву. В штате 45 сотрудников. При проверке выяснилось: 30 сотрудников имеют пароль длиннее 8 символов, 25 сотрудников используют цифры в пароле, 20 сотрудников используют заглавные буквы. При этом 10 сотрудников удовлетворяют всем трем требованиям сразу, 15 сотрудников имеют пароль длиннее 8 символов и используют цифры, но не используют заглавные буквы, а 8 сотрудников используют цифры и заглавные буквы, но имеют пароль короче 8 символов. Сколько сотрудников не удовлетворяют ни одному из трех требований?

5. Прочитайте текст и запишите развернутый ответ. В крупной логистической компании внедрена автоматизированная система управления перевозками, которая обрабатывает маршруты, данные о грузах, персональные данные водителей и клиентов, а также финансовую информацию. Система имеет веб-интерфейс для удаленного доступа диспетчеров. В ходе аудита выявлено, что сотрудники используют единую учетную запись с правами администратора для входа в систему, пароль от которой известен всем диспетчерам и хранится в общем доступе в мессенджере. Кроме того, отсутствует журнал аудита действий пользователей, а удаленный доступ осуществляется по незащищенному протоколу. Определите, какие три базовых свойства информации (из триады CIA) нарушаются в описанной ситуации, и для каждого свойства укажите, какое конкретное действие или упущение в компании приводит к его нарушению.

6. Прочитайте текст и запишите развернутый ответ. В государственном учреждении принято решение о переходе на отечественное программное обеспечение. Закуплены и установлены сертифицированные средства защиты информации, но сотрудники жалуются, что новое ПО работает медленно, часто зависает, и они вынуждены использовать несертифицированные альтернативные программы для выполнения срочных задач. Руководитель службы безопасности требует строгого соблюдения политики безопасности и запрещает использование несертифицированного ПО, а руководители отделов настаивают на необходимости обеспечить непрерывность рабочих процессов. Опишите, какой конфликт целей управления информационной безопасностью возникает в данной ситуации, и как он связан с тремя базовыми свойствами информации.

7. Прочитайте текст и запишите развернутый ответ. В небольшой IT-компании, разрабатывающей мобильные приложения, произошла утечка исходного кода нового продукта, который готовился к выходу на рынок. Расследование показало, что исходный код хранился на облачном файловом хранилище, доступ к которому имели все сотрудники отдела разработки. Один из разработчиков использовал личный аккаунт для синхронизации файлов, но не включил двухфакторную аутентификацию. Его учетная запись была взломана методом подбора пароля (поскольку пароль был простым и использовался им на множестве других сайтов). При этом в компании существовал регламент, требующий использования корпоративных аккаунтов только с двухфакторной аутентификацией, но его выполнение никем не контролировалось, а нарушителя, допустившего утечку, не удалось идентифицировать, так как журналы доступа к облачному хранилищу не велись. Определите, какие организационно-распорядительные меры защиты информации были нарушены в компании. Какие этапы жизненного цикла конфиденциальной информации (создание, обработка, хранение, передача, уничтожение) оказались под угрозой в данном инциденте?

8. Прочитайте текст и запишите развернутый ответ. Медицинская клиника перешла на электронный документооборот и хранит истории болезней пациентов в специализированной медицинской информационной системе. Система имеет следующие характеристики: разграничение прав доступа по ролям (врачи имеют доступ только к своим пациентам, администраторы – к общим данным без диагнозов, руководство – к статистике без идентификаторов), автоматическое логирование всех действий пользователей, шифрование данных при передаче. Однако в ходе проверки выяснилось, что резервное копирование баз данных производится раз в месяц и хранится в том же серверном помещении, что и основной сервер. Также медицинские сестры, работающие за общим компьютером в процедурном кабинете, не выходят из своих учетных записей после завершения работы, и следующий сотрудник может зайти под их именем. Проанализируйте, какие аспекты политики безопасности организации требуют доработки, несмотря на наличие продвинутых технических решений. Опишите, какие риски создает описанный подход к резервному копированию и общий компьютер в процедурном кабинете с точки зрения трех базовых свойств информации.

Итоговый тест

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

1. Какие из перечисленных свойств относятся к триаде базовых свойств информации (модель CIA)?

А) Конфиденциальность
Б) Аутентичность
В) Целостность
Г) Доступность

2. Какие из перечисленных категорий информации относятся к конфиденциальной информации согласно российскому законодательству?

А) Государственная тайна

Б) Коммерческая тайна

В) Общедоступная информация

Г) Персональные данные

3. Что из перечисленного относится к этапам жизненного цикла конфиденциальной информации?

А) Создание документа

Б) Публикация в открытых источниках

В) Обработка и использование

Г) Уничтожение или передача в архив

4. Какие из перечисленных мер относятся к организационно-распорядительным методам защиты информации?

А) Установка межсетевого экрана

Б) Разработка политики безопасности

В) Проведение инструктажей сотрудников

Г) Шифрование данных на диске

5. Какие органы осуществляют сертификацию средств защиты информации в Российской Федерации?

А) ФСТЭК России

Б) ФСБ России

В) Роскомнадзор

Г) Минцифры России

6. Какие из перечисленных действий относятся к методам несанкционированного доступа к информации?

А) Социальная инженерия

Б) Перехват побочных электромагнитных излучений

В) Установка антивирусного ПО

Г) Внедрение программных закладок

7. Какие принципы защиты информации считаются основополагающими при построении системы защиты?

А) Принцип непрерывности защиты

Б) Принцип максимальной сложности паролей

В) Принцип минимальной привилегии

Г) Принцип персональной ответственности

8. Какие риски возникают при использовании общего компьютера несколькими сотрудниками без выхода из учетной записи?

А) Нарушение конфиденциальности информации

Б) Повышение производительности труда

В) Невозможность идентификации нарушителя

Г) Ускорение резервного копирования

9. Какие из перечисленных угроз относятся к угрозам доступности информации?

А) DDoS-атака

Б) Отказ оборудования

В) Перехват пароля

Г) Несанкционированное копирование базы данных

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

10. Какие нормативные правовые акты регулируют защиту информации в Российской Федерации?

А) Федеральный закон "О персональных данных"

Б) Федеральный закон "Об информации, информационных технологиях и о защите информации"

В) ГОСТ Р ИСО/МЭК 27001

Г) Закон РФ "О государственной тайне"

11. Какие элементы включает в себя процесс менеджмента информационной безопасности?

А) Идентификация активов

Б) Оценка рисков

В) Внедрение мер защиты

Г) Только установка антивирусного ПО

12. Какие из перечисленных мероприятий должны проводиться при работе с кадрами для обеспечения информационной безопасности?

А) Проверка благонадежности при приеме на работу

Б) Предоставление безлимитного доступа ко всем данным

В) Ознакомление с политикой безопасности под подпись

Г) Проведение периодических инструктажей

13. Какие последствия могут наступить при нарушении требований законодательства в области защиты персональных данных?

А) Административные штрафы

Б) Уголовная ответственность

В) Отзыв лицензии (для лицензируемых видов деятельности)

Г) Снижение заработной пла14. Какие из перечисленных каналов утечки информации относятся к техническим каналам?

А) Подслушивание переговоров

Б) Чтение документов с экрана монитора соседним сотрудником

В) Перехват побочных излучений компьютера

Г) Использование микрофона в помещении

15. Что из перечисленного характеризует понятие "уязвимость информации" в отличие от "угрозы"?

А) Уязвимость является внутренним недостатком системы

Б) Угроза всегда следствие действий человека

В) Уязвимость может существовать, даже если угроза не реализована

Г) Уязвимость и угроза являются синонимами