СОЧИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
федерального государственного автономного образовательного
учреждения высшего образования
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ»

Отделение среднего профессионального образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

"Основы информационной безопасности"

(наименование дисциплины)

Освоение учебной дисциплины ведется в рамках реализации основной образовательной программы среднего профессионального образования (ОП СПО):

09.02.12 Техническая эксплуатация и сопровождение информационных систем

(код и наименование специальности/профессии ОП СПО)

Квалификация:

специалист по технической эксплуатации и сопровождению информационных систем

(наименование квалификации)

Сочи,
2026 г.

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.06 Основы информационной безопасности

название дисциплины

1.1. Область применения программы

Программа учебной дисциплины ОП.06 Основы информационной безопасности является частью программы подготовки специалистов среднего звена в соответствии с ФГОС "Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ (приказ Минпросвещения России от 10.03.2025 г. № 184)"

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена.

Учебная дисциплина ОП.06 Основы информационной безопасности входит в общепрофесиональный цикл профессиональной подготовки.

1.3. Цели и задачи – требования к результатам освоения учебной дисциплины.

Основная цель – способствовать формированию общих и профессиональных компетенций посредством приобретения знаний, умений и навыков.

В результате освоения учебной дисциплины студент должен знать:

Основные понятия, принципы и цели информационной безопасности.
Виды угроз информационной безопасности и методы их классификации.
Нормативно-правовую базу в области обеспечения информационной безопасности в Российской Федерации (ФЗ №149, ФЗ №152, ФЗ №187 и др.).
Основные модели нарушителя и атак в информационных системах.
Принципы построения и функционирования систем защиты информации.
Методы и средства защиты информации: антивирусные программы, межсетевые экраны, системы обнаружения и предотвращения вторжений.
Основы криптографической защиты информации (шифрование, электронная подпись, хеширование).
Принципы безопасного поведения пользователей в информационных системах и сетях.
Основы обеспечения безопасности при работе с персональными данными.
Подходы к управлению рисками информационной безопасности.

В результате освоения учебной дисциплины студент должен уметь:

Идентифицировать потенциальные угрозы информационной безопасности в типовых ИС.
Применять базовые средства защиты информации (антивирусные программы, брандмауэры, шифрование).
Настраивать параметры безопасности операционных систем и прикладного программного обеспечения.
Реализовывать меры по защите персональных данных в соответствии с требованиями законодательства РФ.
Проводить базовую диагностику уязвимостей и анализировать инциденты информационной безопасности.
Разрабатывать и применять политики информационной безопасности в учебных и производственных проектах.
Обеспечивать безопасность при работе в локальных и глобальных сетях.
Использовать криптографические инструменты для защиты конфиденциальности и

целостности данных.

В результате освоения учебной дисциплины студент должен иметь навыки и (или) опыт деятельности:

Навыками безопасного использования информационных технологий.
Методиками оценки рисков информационной безопасности.
Практическими навыками настройки и администрирования средств защиты информации.
Культурой ответственного и этичного поведения при работе с информацией.
Базовыми компетенциями по реагированию на инциденты информационной безопасности.
Навыками работы с нормативно-правовыми документами в области ИБ.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Объем программы 84 часов, в том числе:
аудиторной учебной нагрузки обучающегося 60 часов;
самостоятельной работы обучающегося 12 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Таблица 1. Виды учебной работы по периодам освоения ООП СПО для формы обучения - очная.

Вид учебной работы	**Всего, ак. ч.**	**Семестр(-ы)**					
		4	**2**				
Контактная (аудиторная) работа (всего)	60	60	34				
в том числе:	-	-	-	-	-	-	-
лекции (если предусмотрено)	24	24	-				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
лабораторные занятия (если предусмотрено)	-	-	-				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
практические занятия (если предусмотрено)	36	36	34				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
Самостоятельная работа обучающегося (всего)	12	12	4				
в том числе:	-	-	-	-	-	-	-
в форме практической подготовки (если предусмотрено)	-	-	-				
Часов на контроль:	12	12	18				
Промежуточная аттестация в форме: (зачет/дифзачет/ экзамен)	-	Эк	Эк				
Общая трудоемкость час	84	84	56				

2.2. Тематический план и содержание учебной дисциплины ОП.06 Основы информационной безопасности

Таблица 2. Содержание дисциплины/МДК по видам учебной работы

НАИМЕНОВАНИЕ РАЗДЕЛА ДИСЦИПЛИНЫ Содержание раздела (темы)	Вид учебной работы*	Кол-во часов
1. Введение в информационную безопасность	**4**	
Основные понятия и определения. История и развитие информационной безопасности.	Лек	2
Актуальные угрозы и риски в информационной безопасности	Пр	2
2. Управление безопасностью информации	**6**	
Нормативно-правовое регулирование в области ИБ.	Лек	2
Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	Лек	2
Политики и процедуры безопасности.	Пр	2
3. Криптография	**8**	
Основы криптографии: симметричные и асимметричные алгоритмы.	Лек	2
Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	Лек	2
Работа с симметричными и асимметричными алгоритмами	Пр	2
Хэширование и создание цифровой подписи сообщения	Пр	2
4. Защита сетевой инфраструктуры	**6**	
Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.)	Лек	1
Использование VPN и межсетевых экранов	Лек	1
Организация защиты от атак	Пр	2
Организация работы VPN и межсетевого экрана	Пр	2
5. Безопасность приложений	**4**	
Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики	Лек	2
Тестирование на проникновение и анализ уязвимостей.	Пр	2
6. Защита данных	**6**	
Шифрование данных в покое и в транзите.	Лек	1
Резервное копирование и восстановление данных. Управление доступом к данным	Лек	1
Выполнение резервного копирования и восстановления данных	Пр	2
Управление доступом к данным	Пр	2
7. Безопасность облачных технологий	**6**	
Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	Лек	2
Изучение модели облачных услуг и их безопасности	Пр	4
8. Инциденты безопасности	**10**	
Реакция на инциденты и управление ими	Пр	2
Анализ инцидентов и цифровая криминалистика	Пр	2
Восстановление после инцидента.	Пр	2
Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	Лек	2
Работа с инцидентами	Пр	2

9. Социальная инженерия и человеческий фактор	**6**	
Психология атак: социальная инженерия	Лек	2
Обучение сотрудников информационной безопасности	Пр	2
Разработка политики информационной безопасности	Пр	2
10. Будущее информационной безопасности	**4**	
Тенденции и новые технологии в области безопасности (AI, ML, блокчейн)	Лек	2
Этические аспекты информационной безопасности	Пр	2
Промежуточная аттестация	**24**	
Экзамен	Эк	12
Самостоятельная работа по разделам. Подготовка к аттестации	СР	12

** - Лек – лекции; Пр – практические занятия; СР – самостоятельная работа; ЛР – лабораторные работы.*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены специальные помещения, приведенным в п 6.3 основной образовательной программы специальности.

Таблица 3. Материально-техническое обеспечение дисциплины

Тип аудитории	**Оснащение аудитории** **Специализированное учебное оборудование, ПО и материалы для освоения дисциплины (при необходимости)**
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (компьютерный класс)	Комплект специализированной мебели; доска аудиторная меловая; технические средства: автоматизированные рабочие места (процессор не ниже AMD Ryzen 3, оперативная память объемом не менее 8Гб; HDD память объемом не менее 500 gb) в количестве 11 штук, проектор BenQ MS521P, проекционный экран Lumien Master Picture. Имеется выход в интернет. Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный
Аудитория для самостоятельной работы обучающихся	Комплект специализированной мебели; Телевизор LED LG 42", автоматизированные рабочие места (процессор не ниже AMD Quad-Core, оперативная память объемом не менее 4Гб; HD500gb), имеется выход в интернет Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Щербак А. В. Информационная безопасность : учебник для спо. - Москва: Юрайт, 2024. - 259 с - Текст : электронный. - URL: https://urait.ru/bcode/543873

Дополнительные источники:

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:

- Электронно-библиотечная система BOOK.RU https://book.ru/
- Электронно-библиотечная система РУДН – ЭБС РУДН http://mega.rudn.ru/MegaPro/Web
- ЭБС Znanium https://znanium.ru
- Образовательная платформа Юрайт https://urait.ru

2. Базы данных и поисковые системы:

- Учебный портал института https://portal.rudn-sochi.ru/

Методические материалы для обучающихся

Формирование содержания учебной дисциплины осуществлялся на основе следующих принципов:
- учет возрастных особенностей обучающихся,
- практическая направленность обучения;
- дифференцированный и индивидуальный подход
- формирование знаний, которые обеспечат обучающимся колледжа успешную адаптацию к профессиональной деятельности.

Самостоятельная работа студента является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.

Правильно спланированная и организованная самостоятельная работа студентов позволяет:
-сделать образовательный процесс более качественным и интенсивным;
-способствует созданию интереса к избранной профессии и овладению ее особенностями;
-приобщить студента к творческой деятельности;
-проводить в жизнь дифференцированный подход к обучению.

При организации самостоятельной работы студентов в качестве методологической основы должен применяться деятельный подход, когда обучение ориентировано на формирование умений решать не только типовые, но и нетиповые задачи, когда студент должен проявить творческую активность, инициативу, знания, умения и навыки, полученные при изучении конкретной дисциплины.

Учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины на Учебном портале.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Таблица 4. Контроль и оценка результатов освоения дисциплины

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**

Знания: Основные понятия, принципы и цели информационной безопасности. Виды угроз информационной безопасности и методы их классификации. Нормативно-правовую базу в области обеспечения информационной безопасности в Российской Федерации (ФЗ №149, ФЗ №152, ФЗ №187 и др.). Основные модели нарушителя и атак в информационных системах. Принципы построения и функционирования систем защиты информации. Методы и средства защиты информации: антивирусные программы, межсетевые экраны, системы обнаружения и предотвращения вторжений. Основы криптографической защиты информации (шифрование, электронная подпись, хеширование). Принципы безопасного поведения пользователей в информационных системах и сетях. Основы обеспечения безопасности при работе с персональными данными. Подходы к управлению рисками информационной безопасности.	Анализ и оценка выполнения индивидуальных заданий, расчетных работ, опрос, тематический диктант, контрольная работа, практические занятия, домашние работы, компьютерное тестирование, Взаимоконтроль и самоконтроль студентов. Полнота и грамотность подготовленных докладов, сообщений, презентаций.
Умения: Идентифицировать потенциальные угрозы информационной безопасности в типовых ИС. Применять базовые средства защиты информации (антивирусные программы, брандмауэры, шифрование). Настраивать параметры безопасности операционных систем и прикладного программного обеспечения. Реализовывать меры по защите персональных данных в соответствии с требованиями законодательства РФ. Проводить базовую диагностику уязвимостей и анализировать инциденты информационной безопасности. Разрабатывать и применять политики информационной безопасности в учебных и производственных проектах. Обеспечивать безопасность при работе в локальных и глобальных сетях. Использовать криптографические инструменты для защиты конфиденциальности и целостности данных.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, беседа, опрос, практические занятия, домашние работы, компьютерное тестирование

Практический опыт: Навыками безопасного использования информационных технологий. Методиками оценки рисков информационной безопасности. Практическими навыками настройки и администрирования средств защиты информации. Культурой ответственного и этичного поведения при работе с информацией. Базовыми компетенциями по реагированию на инциденты информационной безопасности. Навыками работы с нормативно-правовыми документами в области ИБ.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, выполнение и защита индивидуальных заданий.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 5. Перечень компетенций

Шифр	Результаты (компетенции) Основные показатели результатов подготовки
ОК 05.	**Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста**
Знать: правила оформления документовправила построения устных сообщенийособенности социального и культурного контекста	
Уметь: грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языкепроявлять толерантность в рабочем коллективе	
ОК 09.	**Пользоваться профессиональной документацией на государственном и иностранном языках**
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности.	
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы.	
ПК 1.1.	**Осуществлять сбор данных для выявления требований к типовой информационной системе в соответствии с техническим заданием**

Знать: возможности типовой ИС; предметную область автоматизации; инструменты и методы выявления требований к ИС; технологии межличностной и групповой коммуникации в деловом взаимодействии, основы конфликтологии; архитектуру, устройство и функционирование вычислительных систем; коммуникационное оборудование; сетевые протоколы; основы современных операционных систем; основы современных систем управления базами данных (далее - СУБД); устройство и функционирование современных ИС; основы архитектуры мультиарендного программного обеспечения; основы ИБ организации; современные стандарты информационного взаимодействия систем; программные средства и платформы инфраструктуры информационных технологий организаций; системы классификации и кодирования информации, в том числе присвоения кодов документам и элементам справочников; отраслевую нормативно-техническую документацию; источники информации, необходимой для профессиональной деятельности в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; лучшие практики создания (модификации) и сопровождения ИС в экономике; основы бухгалтерского учета и отчетности организаций; основы налогового законодательства Российской Федерации; культуру речи; правила деловой переписки.	
Уметь: осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; разрабатывать документы, необходимые для технической поддержки процессов создания (модификации) и сопровождения ИС.	
Владеть: сбора в соответствии с трудовым заданием документации заказчика, связанной с его потребностями и запросами к типовой ИС; анкетирования представителей заказчика в соответствии с трудовым заданием для выявления требований к типовой ИС; интервьюирования представителей заказчика в соответствии с трудовым заданием для выявления требований к типовой ИС; документирования собранных для выявления требований заказчика к типовой ИС данных в соответствии с регламентами организации.	
ПК 1.7.	**Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем**
Знать: основы ИБ организации; модель угроз информационной безопасности ИС организации заказчика; процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика; основы администрирования СУБД; основы системного администрирования; коммуникационное оборудование; сетевые протоколы; основы современных операционных систем; устройство и функционирование современных ИС; основы архитектуры мультиарендного программного обеспечения.Администрирование баз данных	

Уметь: идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС.	
Владеть: распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; передачи информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; информирования заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; временного блокирования доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС.	
ПК 2.1.	**Осуществлять подготовку тестовых данных в соответствии с заданием на тестирование программного обеспечения**
Знать: основные средства резервного копирования данных и их возможности; основы операционных систем; основные средства работы с жесткими дисками; типовой алгоритм проведения процедуры резервного копирования; основы систем управления БД; основные средства контроля целостности данных; типовой алгоритм процедуры восстановления данных; основы операционных систем	
Уметь: создавать расписание резервного копирования данных; вычислять размер полной резервной копии БД; читать техническую документацию на БД; работать с устройствами резервного копирования данных и носителями резервных копий; выполнять регламентные процедуры по резервированию данных; проверять восстановимость резервной копии данных; читать техническую документацию на БД; выполнять регламентные процедуры по восстановлению данных; осуществлять проверку корректности восстановленных данных.	
Владеть: планирования процедур резервного копирования данных; запуска процедуры резервного копирования данных; мониторинга выполнения процедур резервного копирования данных; контроля завершения процедуры резервного копирования данных; проведения повторной процедуры резервного копирования данных в случае ее нештатного завершения; хранения резервных копий БД; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; проведения повторной процедуры восстановления БД в случае ее нештатного завершения	
ОК 02.	**Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности**

Знать: номенклатура 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 цифровые средства.	
Уметь: определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач.	
ОК 04.	**Эффективно взаимодействовать и работать в коллективе и команде**
Знать: психологические основы деятельности коллективапсихологические особенности личности	
Уметь: организовывать работу коллектива и командывзаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	
ПК 2.1.	**Выполнять подготовку данных для проведения аналитических работ**
Знать: основные средства резервного копирования данных и их возможности; основы операционных систем; основные средства работы с жесткими дисками; типовой алгоритм проведения процедуры резервного копирования; основы систем управления БД; основные средства контроля целостности данных; типовой алгоритм процедуры восстановления данных; основы операционных систем	
Уметь: создавать расписание резервного копирования данных; вычислять размер полной резервной копии БД; читать техническую документацию на БД; работать с устройствами резервного копирования данных и носителями резервных копий; выполнять регламентные процедуры по резервированию данных; проверять восстановимость резервной копии данных; читать техническую документацию на БД; выполнять регламентные процедуры по восстановлению данных; осуществлять проверку корректности восстановленных данных.	
Владеть: планирования процедур резервного копирования данных; запуска процедуры резервного копирования данных; мониторинга выполнения процедур резервного копирования данных; контроля завершения процедуры резервного копирования данных; проведения повторной процедуры резервного копирования данных в случае ее нештатного завершения; хранения резервных копий БД; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; проведения повторной процедуры восстановления БД в случае ее нештатного завершения	
ПК 2.1.	**Оформлять техническую документацию на продукцию в сфере информационно-коммуникационных технологий**

Знать: основные средства резервного копирования данных и их возможности; основы операционных систем; основные средства работы с жесткими дисками; типовой алгоритм проведения процедуры резервного копирования; основы систем управления БД; основные средства контроля целостности данных; типовой алгоритм процедуры восстановления данных; основы операционных систем	
Уметь: создавать расписание резервного копирования данных; вычислять размер полной резервной копии БД; читать техническую документацию на БД; работать с устройствами резервного копирования данных и носителями резервных копий; выполнять регламентные процедуры по резервированию данных; проверять восстановимость резервной копии данных; читать техническую документацию на БД; выполнять регламентные процедуры по восстановлению данных; осуществлять проверку корректности восстановленных данных.	
Владеть: планирования процедур резервного копирования данных; запуска процедуры резервного копирования данных; мониторинга выполнения процедур резервного копирования данных; контроля завершения процедуры резервного копирования данных; проведения повторной процедуры резервного копирования данных в случае ее нештатного завершения; хранения резервных копий БД; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; проведения повторной процедуры восстановления БД в случае ее нештатного завершения	
ПК 2.1.	**Выполнять резервное копирование и восстановление данных в штатном режиме**
Знать: основные средства резервного копирования данных и их возможности; основы операционных систем; основные средства работы с жесткими дисками; типовой алгоритм проведения процедуры резервного копирования; основы систем управления БД; основные средства контроля целостности данных; типовой алгоритм процедуры восстановления данных; основы операционных систем	
Уметь: создавать расписание резервного копирования данных; вычислять размер полной резервной копии БД; читать техническую документацию на БД; работать с устройствами резервного копирования данных и носителями резервных копий; выполнять регламентные процедуры по резервированию данных; проверять восстановимость резервной копии данных; читать техническую документацию на БД; выполнять регламентные процедуры по восстановлению данных; осуществлять проверку корректности восстановленных данных.	

Владеть: планирования процедур резервного копирования данных; запуска процедуры резервного копирования данных; мониторинга выполнения процедур резервного копирования данных; контроля завершения процедуры резервного копирования данных; проведения повторной процедуры резервного копирования данных в случае ее нештатного завершения; хранения резервных копий БД; запуска процедуры восстановления БД; мониторинга выполнения процедуры восстановления БД; контроля завершения процедуры восстановления БД; проведения повторной процедуры восстановления БД в случае ее нештатного завершения	
ПК 2.2.	**Управлять доступом к базам данных**
Знать: основные положения теории БД, хранилищ данных, баз знаний; методы и средства технической защиты информации; технологии передачи данных и обмена данными в компьютерных сетях; способы контроля доступа к данным и управления привилегиями.	
Уметь: выполнять процедуры управления правами доступа пользователей к БД; выявлять случаи нарушения прав доступа пользователей к БД.	
Владеть: назначения прав доступа пользователей к БД; изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД.	
ПК 2.5.	**Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных**
Знать: понятие и классификация инцидентов ИБ; типичные угрозы ИБ при работе с БД; процедуры и регламенты передачи информации об инцидентах в службу ИБ организации; средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры); основы работы со средствами антивирусной защиты; основы ИБ; основы деловой этики; правила деловой переписки.	
Уметь: идентифицировать инциденты ИБ при работе с БД; осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации); управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ; устанавливать и сопровождать антивирусное ПО.	
Владеть: распознавания инцидентов ИБ при работе с БД; формирования перечня инцидентов ИБ; передачи информации об инцидентах в службу ИБ организации; временного блокирования доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости); поддержания баз антивирусных программ в актуальном состоянии.	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Основы информационной безопасности»

Перечень вопросов для подготовки к занятиям и промежуточной аттестации, контрольных работ, содержание заданий для выполнения практических и самостоятельных работ, рекомендации по выполнению и критерии оценивания представлены в фонде оценочных средств по дисциплине «Основы информационной безопасности» в Приложении к настоящей Рабочей программе дисциплины.

Оценочные средства позволяют провести текущий контроль по дисциплине. По каждому средству оценивается полнота и глубина освоения, характеризующиеся показателями и критериями оценивания

Таблица 6. Показатели и критерии оценивания

Показатель	Критерий
Пороговый (узнавание) «3»	Знает: базовые общие знания; Умеет: основные умения, требуемые для выполнения простых задач; Владеет: работает при прямом наблюдении.
Базовый (воспроизведение) «4»	Знает: факты, принципы, процессы, общие понятия в пределах области исследования; Умеет: диапазон практических умений, требуемых для решения определенных проблем в области исследования; Владеет: берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Высокий (компетентность) «5» max балл	Знает: фактическое и теоретическое знание в пределах области исследования с пониманием границ применимости; Умеет: диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем; Владеет: контролирует работу, проводит оценку, совершенствует действия работы

Максимальное количество баллов по каждому оценочному средству соответствует вербальному критерию «высокий».

7. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

7.1 Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

В процессе обучения используются активные и интерактивные образовательные технологии (формы проведения занятий):

-лекции, фронтальные опросы, презентации и защита мини-проектов;

-кейс-стади (разбор конкретных ситуаций),

-имитационные компьютерные модели;

-организации самостоятельной учебно-познавательной деятельности (индивидуальные домашние задания).