Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«28» 11 2025 г.

Рабочая программа учебной дисциплины

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности:
09.02.12 Техническая эксплуатация и сопровождение информационных систем

Квалификация: специалист по технической эксплуатации и сопровождению информационных систем

Год начала подготовки: 2026

Екатеринбург
2025

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___» _____ 2025 г.

Рабочая программа учебной дисциплины

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности:
09.02.12 Техническая эксплуатация и сопровождение информационных систем

Квалификация: специалист по технической эксплуатации и сопровождению информационных систем

Год начала подготовки: 2026

Екатеринбург
2025

Рабочая программа учебной дисциплины разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, утвержденным приказом Министерства просвещения Российской Федерации от 10 марта 2025 г. № 184.

Программу составил:
Каменсков А.Е. - преподаватель ЦК ЭТД кафедры ИТиМС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол 3 от 26.11.25
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Рабочая программа учебной дисциплины разработана в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, утвержденным приказом Министерства просвещения Российской Федерации от 10 марта 2025 г. № 184.

Программу составил:
Каменсков А.Е. - преподаватель ЦК ЭТД кафедры ИТиМС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности»: формирование у обучающихся знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

1.2 Планируемые результаты освоения дисциплины

При организации процесса изучения дисциплины преподаватель создает образовательное пространство для формирования и развития у обучающихся общих и профессиональных компетенций:

1.2.1 Общие компетенции:

Код ОК	Наименование ОК
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2.2 Профессиональные компетенции:

Код ПК	Наименование ПК
ПК 1.7	Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем.
ПК 2.5	Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных

1.2.3 В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК 01	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её со-	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем	

	ставные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составлять план действия; определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).	в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.	
ОК 02	- 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.	- 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 с использованием цифровых средств.	

ОК 09	- понимать тексты на базовые профессиональные темы.	- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности.	
ПК 1.7	- 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.	- 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.	- распознавание инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; - передача информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; - информирование 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; - временное блокирование доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС.
ПК 2.5	- 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 эле-	- 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);	- распознавание инцидентов ИБ при работе с БД; - формирование перечня инцидентов ИБ; - передача информации об инцидентах в службу ИБ организации; - временное блокирование доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости);

	ментам БД при обнаружении инцидентов ИБ; - устанавливать и сопровождать антивирусное ПО.	- основы работы со средствами антивирусной защиты; - основы ИБ; - основы деловой этики; - правила деловой переписки.	- поддержание баз антивирусных программ в актуальном состоянии.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Трудоемкость освоения дисциплины

Вид учебной работы	Объем часов
Объем учебной дисциплины	**64**
в т.ч. в форме практической подготовки	20
Самостоятельная работа	**8**
Суммарная учебная нагрузка во взаимодействии с преподавателем	**56**
в том числе:	
- теоретическое обучение	28
- лабораторные работы	-
- практические занятия	20
- консультации	2
- промежуточная аттестация (экзамен)	6

2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, ак.ч. / в т.ч. в форме практической подготовки, ак.ч.	Коды компетенций, формированию которых способствует элемент программы
1	**2**	**3**	**4**
Раздел 1 Фундаментальные основы и управление информационной безопасностью.		**6/-**	
Тема 1.1 Введение в информационную безопасность.	**Содержание учебного материала:** 1 Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности.	2	ОК 01, ОК 02, ОК 09
Тема 1.2 Управление безопасностью информации.	**Содержание учебного материала:** 1 Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.).	2	ОК 01, ОК 02, ОК 09
Тема 1.3 Будущее информационной безопасности.	**Содержание учебного материала:** 1 Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.	2	ОК 01, ОК 02, ОК 09

Раздел 2 Криптографические методы и защита данных.		**18/8**	
Тема 2.1 Криптография.	**Содержание учебного материала:** 1 Понятие криптографии. История ее возникновения. Понятие шифра. Методы создания шифротекста: перестановки, замены, One-Time Pad. Понятие криптоанализа. Методы взламывания кода. 2 Понятие хэш-функции. Область ее использования. Свойства хэш-функций. Алгоритмы хэширования: MD5 и SHA. Их реализация, сравнительная характеристика. Использование хэш-функций для аутентификации устройств. Алгоритм HMAC, принцип его реализации.	2 2	ОК 01, ОК 02, ОК 09
	Практические занятия: 1 Работа с симметричными и асимметричными алгоритмами. 2 Хэширование и создание цифровой подписи сообщения.	2 2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Тема 2.2 Защита данных.	**Содержание учебного материала:** 1 Назначение криптографических ключей. Основные характеристики управления ключами: генерация, проверка, обмен, хранение, время жизни, отзыв и уничтожение. Понятие длины и пространства ключей. Типы криптографических ключей: симметричные, ассиметричные, цифровая подпись, хэш. Критерии выбора ключей. 2 Понятие шифрования. Виды алгоритмов шифрования: симметричные и асимметричные. Их сравнительная характеристика. Основные принципы реализации. Алгоритмы симметричного и асиметричного шифрования, их сравнительная характеристика.	2 2	ОК 01, ОК 02, ОК 09
	Практические занятия: 3 Выполнение резервного копирования и восстановления данных. 4 Управление доступом к данным.	2 2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
	Самостоятельная работа: 1 Оформление отчетов по практическим занятиям.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Раздел 3 Технические средства защиты инфраструктуры и приложений.		**20/8**	
Тема 3.1 Защита сетевой инфраструктуры.	**Содержание учебного материала:** 1 Понятие сетевой атаки. Виды атак: sniffing, IP-spoofing, DoS, парольная атака, Man-in-the-Middle, сетевая разведка, злоупотребление доверием, социальная инженерия. Механизмы атаки, методы защиты от них. 2 Принцип реализации атак на канальном и сетевом уровне: переполнение таблицы адресов, ARP-spoofing, атаки на протоколы IEEE 802.1Q, STP, DHCP. Методы защиты.	2 2	ОК 01, ОК 02, ОК 09

	Практические занятия: 5 Организация защиты от атак на сетевую инфраструктуру.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Тема 3.2 Защита оконечного оборудования сетевой инфраструктуры.	**Содержание учебного материала:** 1 Понятие вирусов. Классификация вирусов: Их особенности, принцип действия, наносимый вред. Методы проникновения вирусов в компьютер. Признаки наличия вирусов в компьютере. Методы защиты компьютеров от проникновения вирусов. Понятие антивирусной программ. Требования предъявляемые антивирусным программы. Виды антивирусных программ: Их особенности и принцип работы.	2	ОК 01, ОК 02, ОК 09
Тема 3.3 Безопасность приложений.	**Содержание учебного материала:** 1 Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	ОК 01, ОК 02, ОК 09
	Практические занятия: 6,7 Анализ уязвимостей приложений в сетевой инфраструктуре.	4	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Тема 3.4 Безопасность облачных технологий.	**Содержание учебного материала:** 1 Понятие облачных сред. Их особенности. Модели облачных услуг (IaaS, PaaS, SaaS), принцип их реализации. Особенности безопасности в облачных средах.	2	ОК 01, ОК 02, ОК 09
	Практические занятия: 8 Исследование безопасности различных облачных моделей.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
	Самостоятельная работа: 1 Оформление отчетов по практическим занятиям.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Раздел 4 Реагирование на угрозы и человеческий фактор.		**12/4**	
Тема 4.1 Инциденты безопасности.	**Содержание учебного материала:** 1 Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.	2	ОК 01, ОК 02, ОК 09
	Практические занятия: 9 Исследование и анализ инцидентов в области сетевой безопасности.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Тема 4.2 Социальная инженерия и человеческий фактор.	**Содержание учебного материала:** 1 Понятие психологической атаки. Виды психологических атак: социальная инженерия и фишинг. Их разновидности. Понятие политики безопасности сетей предприятия. Основные разделы, их состав. Обеспечение соблюдения политики безопасности на предприятии. Последствия ее нарушения.	2	ОК 01, ОК 02, ОК 09

	Практические занятия: 10 Разработка политики информационной безопасности на предприятии.	2	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
	Самостоятельная работа: 1 Оформление отчетов по практическим занятиям. 2 Подготовка к экзамену.	4	ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5
Консультации:		**2**	
Промежуточная аттестация:		**6**	
Всего:		**64/20**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение

Для реализации дисциплины предусмотрены следующие специальные помещения, оснащенные оборудованием и техническими средствами обучения:

3.1.1 Учебная аудитория V УК №3:

Комплект специализированной учебной мебели (столы и стулья - рабочие места обучающихся и преподавателя), доска аудиторная; персональный компьютер, проектор, экран для проектора.

Выход в Интернет и доступ в электронную информационно-образовательную среду организации.

Программное обеспечение: Kaspersky Endpoint Security; Google Chrome; PDF24; Foxit PDF Reader; FastStone; VLC; 7ZIP; МойОфис; AnyLogic Education; Консультант+; DjVU Reader; DosBox; SMathStudio; VirtualBox; Компас 3D; MongoDB Compass; Microsoft SSMS; Sublime Text; VirtualBox; Virtual Studio; Visual Studio Code; SWI-Prolog; Teams; WampServer; WinDjView; Консультант+; Операционная система Linux (свободно распространяемая, лицензия GNU GPL).

3.1.2 Лаборатория «Компьютерных сетей и основ информационной безопасности» 205 УК №3:

Комплект специальной учебной мебели (столы и стулья - рабочие места обучающихся и преподавателя), магнитно-маркерная доска.

Лабораторное оборудование: коммутатор Catalyst 2960-XR Series; коммутатор Catalyst 2960 Series; маршрутизатор Cisco 2901; маршрутизатор Cisco 3925; ноутбуки.

Выход в Интернет и доступ в электронную информационно-образовательную среду организации, в том числе с рабочих мест обучающихся.

Программное обеспечение: Kaspersky Endpoint Security; Google Chrome; PDF24; Foxit PDF Reader; FastStone; VLC; 7ZIP; МойОфис; AnyLogic Education; Arduino IDE; Eclipse; Eclipse; Beekeeper Studio; DjVU Reader; DosBox; GNS3 (Graphical Network Simulator); GPSS World Core (Студенческая версия); GPSS Studio; SMathStudio; VirtualBox; InkScape; IntellijIDEA; OpenJDK; Krita; LISP; MicroSIP; MongoDB Compass; Mozilla Firefox; MySQL Server; Node.js; Notepad++; Postman; PostgreSQL; PuTTY; PyCharm Community; QT Designer; Ramus; Scilab; Microsoft SSMS; Sublime Text; Teams; VirtualBox; Virtual Studio; Visual Studio Code; WampServer; WinDjView; WireShark; NanoCAD +; XAMPP; FileZilla; Blender; Операционная система Linux (свободно распространяемая, лицензия GNU GPL).

3.1.3 Кабинет самостоятельной работы 417 УК №3:

Комплект специализированной учебной мебели (столы и стулья - рабочие места обучающихся и преподавателя), доска аудиторная, персональные компьютеры.

Выход в Интернет и доступ в электронную информационно-образовательную среду организации, в том числе с рабочих мест обучающихся.

Программное обеспечение: Kaspersky Endpoint Security; Google Chrome; PDF24; Foxit PDF Reader; FastStone; VLC; 7ZIP; МойОфис; Android Studio; AnyLogic Education; Arduino IDE; Eclipse; Eclipse; Консультант+; Beekeeper Studio; DjVU Reader; DosBox; GNS3 (Graphical Network Simulator); GPSS World Core (Студенческая версия); GPSS Studio; SMathStudio; VirtualBox; Компас 3D; InkScape; Multisim. IntellijIDEA; OpenJDK; Krita; LISP; MicroSIP; MongoDB Compass; Mozilla Firefox; MySQL Server; MySQL Workbench; Node.js; Notepad++; Postman; PostgreSQL; PuTTY; PyCharm Community; QT Designer; Ramus; Scilab; Microsoft SSMS; Sublime Text; Teams; VirtualBox; Virtual Studio; Visual Studio Code; WampServer; WinDjView; WireShark; NanoCAD +; XAMPP; FileZilla; Blender; Операционная система Linux (свободно распространяемая, лицензия GNU GPL).

3.2 Учебно-методическое обеспечение

Для реализации дисциплины библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе:

3.2.1 Основные печатные и/или электронные издания:

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547.

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950.

3.2.2 Дополнительные издания:

1. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510.

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Умеет: - распознавать задачу и/или проблему в профессиональном и/или социальном контексте; - анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - 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;	- может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; - анализирует задачу и/или проблему и может выделить её составные части; - умеет определять этапы решения задачи; - может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составляет план действия; - может определять необходимые ресурсы; - владеет актуальными методами работы в профессиональной и смежных сферах; - может реализовывать составленный план; - оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); - умеет определять задачи для поиска информации; - умеет определять необходимые источники информации; - планирует процесс поиска; - умеет структурировать получаемую информацию; - может выделить наиболее значимое в перечне информации; - умеет оценивать практическую значимость результатов поиска; - оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; - может использовать современное программное обеспечение;	- наблюдение выполнения лабораторных работ; - тестирование; - дифференцированный зачет.

- использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	- может использовать различные цифровые средства для решения профессиональных задач; - понимает тексты на базовые профессиональные темы; - умеет шифровать данные и обеспечивать их конфиденциальность; - умеет анализировать требования безопасности информационных систем; - может разрабатывать и реализовывать меры безопасности; - может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	
Знает: - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности; - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности, в том числе с ис-	- ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; - владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; - знает алгоритмы выполнения работ в профессиональной и смежных областях; - знает методы работы в профессиональной и смежных сферах; - знает структуру плана для решения задач; - может произвести оценку результатов решения задач профессиональной деятельности; - владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; - знает приемы структурирования информации; - знает формат оформления результатов поиска информации, современные средства и устройства информатизации; - может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности, в том числе с использова-	

пользованием цифровых средств; - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения данных; - методы защиты баз данных от внешних угроз; - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; - законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и	нием цифровых средств; - владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; - знает принципы безопасности хранения данных; - владеет методами защиты баз данных от внешних угроз; - знает принципы криптографии и методов шифрования данных; - ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; - законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - знает современный отечественный и зарубежный опыт в профессиональной деятельности; - владеет принципами и методами обеспечения безопасности информационных систем; - знает принципы безопасности информационных систем; - владеет современными методами и технологиями в области безопасности информационных систем; - знает законодательные и нормативные акты в области безопасности информационных систем; - знает источники угроз информационной безопасности и меры по их предотвращению; - знает об основных угрозах безопасности мобильных приложений; - ориентируется в принципах криптографии и шифрования данных; - знает стандарты и протоколы безопасности, такие как HTTPS,	

OpenID Connect; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа уязвимости и мониторинга безопасности; - основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; - инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.	OAuth и OpenID Connect; - знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - владеет основными принципами безопасности информации и методов ее защиты; - знает стандартные криптографические алгоритмы для шифрования данных; - имеет представление о принципах обеспечения безопасности передачи данных по сети; - знает основы безопасности приложений и инфраструктуры; - знает методы анализа уязвимости и мониторинга безопасности; - знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; - знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.	