

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Казанский национальный исследовательский технологический
университет»
КАЗАНСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
(ФГБОУ ВО "КНИТУ" КТК)

УТВЕРЖДАЮ

Зам. директора по УР

Р.А. Газизов

«28» марта 2026 г.



РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности
(индекс, название учебной дисциплины)

по специальности 09.02.11 Разработка и управление программным обеспечением
(шифр, специальность)

Казань, 2026

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Минпросвещения России от 24.02.2025 г. № 138.

Составитель (ли): _____

Рабочая программа учебной дисциплины рассмотрена и утверждена на заседании предметно-цикловой комиссии общепрофессиональных дисциплин и профессиональных модулей специальности 09.02.11 Разработка и управление программным обеспечением КТК ФГБОУ ВО "КНИТУ", Протокол № 7 от «27» марта 2026 г.

Председатель ПЦК/ З.Н. Гатятуллина
(ФИО)

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
1.2. Планируемые результаты освоения дисциплины	4
2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
2.1 Объем учебной дисциплины и виды учебной работы.....	11
2.2. Тематический план и содержание предмета	12
3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ.....	14
3.1. Материально-техническое обеспечение.....	14
3.2. Учебно-методическое обеспечение.....	14
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	15

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности» - формирование у обучающихся системы знаний об угрозах информационной безопасности, развитие логического и критического мышления, алгоритмической культуры, способности выявлять каналы утечки информации и применять методы защиты, необходимые для будущей профессиональной деятельности.

Дисциплина «Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

В результате освоения дисциплины обучающийся должен:

<i>Код ОК</i>	Уметь	Знать
ОК.01	<ul style="list-style-type: none">– распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части– определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы– выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы– владеть актуальными методами работы в профессиональной и смежных сферах– оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	<ul style="list-style-type: none">– актуальный профессиональный и социальный контекст, в котором приходится работать и жить– структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях– основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте– методы работы в профессиональной и смежных сферах– порядок оценки результатов решения задач профессиональной деятельности
ОК.02	<ul style="list-style-type: none">– определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации– выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять	<ul style="list-style-type: none">– номенклатура информационных источников, применяемых в профессиональной деятельности– приемы структурирования информации– формат оформления результатов поиска информации– современные средства и устройства информатизации,

	<p>результаты поиска</p> <ul style="list-style-type: none"> – 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 	<p>порядок их применения и</p> <ul style="list-style-type: none"> – программное обеспечение в профессиональной деятельности, в том числе цифровые средства
ОК.09	<ul style="list-style-type: none"> – 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 	<ul style="list-style-type: none"> – 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
ПК.1.1	<ul style="list-style-type: none"> – анализировать предметную область и выделять основные сущности; – определять требования к базе данных; – разрабатывать концептуальную, логическую и физическую модели баз данных; – проектировать схему базы данных; – работать с современными case-средствами проектирования баз данных; – определять связи между таблицами; – определять типы данных для 	<ul style="list-style-type: none"> – основные положения теории баз данных, хранилищ данных, баз знаний; – основные принципы структуризации и нормализации базы данных; – основные принципы построения концептуальной, логической и физической модели данных; – методы описания схем баз данных в современных системах управления базами данных; – структуру данных систем управления базами данных, основные понятия и принципы проектирования баз данных;

	<p>полей таблиц;</p> <ul style="list-style-type: none"> – оформление документации на спроектированную базу данных – разработки схемы базы данных, используя NoSQL модели данных, такие как документо-ориентированные, ключ-значение, колоночные и др. 	<ul style="list-style-type: none"> – структуру реляционной базы данных; – язык SQL и особенности его реализации в различных системах управления базами данных; – оптимизацию производительности баз данных – принципы безопасности хранения данных
ПК.1.4	<ul style="list-style-type: none"> – устанавливать и настраивать СУБД; – создавать и удалять базы данных; – создавать пользователей и назначать права доступа; – оптимизировать запросы к базе данных; – обеспечивать безопасность баз данных; – создавать и настраивать базы данных в соответствии с требованиями бизнеса; – управлять транзакциями и контролировать целостность данных; – обеспечивать безопасность и управлять доступом к данным; – создавать и восстанавливать резервные копии данных; – работать с индексами и оптимизировать производительность запросов; – нормализовать базы данных и проектировать эффективные структуры данных; – мониторить и анализировать производительность баз данных; – работать с нереляционными базами данных и выбирать наиболее подходящий тип базы данных для конкретной задачи 	<ul style="list-style-type: none"> – архитектуру СУБД; – основные принципы администрирования баз данных; – методы мониторинга и оптимизации работы баз данных; – принципы резервного копирования и восстановления баз данных; – методы защиты баз данных от внешних угроз; – особенности работы с различными СУБД; – Язык SQL (Structured Query Language); – управление транзакциями и контроль целостности данных; – управление доступом и безопасностью баз данных; – резервное копирование и восстановление данных; – оптимизацию производительности баз данных; – работу с индексами и оптимизация запросов; – мониторинг и анализ производительности; – принципы работы с реляционными базами данных; – принципы работы с нереляционными базами данных
ПК.1.5	<ul style="list-style-type: none"> – разрабатывать и внедрять системы защиты баз данных от несанкционированного доступа; – разрабатывать и внедрять системы резервного копирования и восстановления баз данных; – проводить аудит безопасности баз 	<ul style="list-style-type: none"> – методы защиты баз данных от несанкционированного доступа; – методы создания и восстановления резервных копий баз данных; – особенности работы с различными типами СУБД;

	<p>данных;</p> <ul style="list-style-type: none"> – устанавливать и настраивать механизмы аутентификации и авторизации пользователей; – создавать и управлять ролями и правами доступа к данным; – шифровать данные и обеспечивать их конфиденциальность; – контролировать целостность данных и обнаруживать изменения; – использовать механизмы аудита для отслеживания доступа к данным; – использовать механизмы мониторинга для обнаружения угроз безопасности; – создавать и управлять защищенными соединениями с базой данных; – использовать механизмы защиты от SQL-инъекций и других видов атак; – создавать и управлять бэкапами и резервными копиями данных; – обеспечивать безопасность базы данных при использовании облачных 	<ul style="list-style-type: none"> – методы проведения аудита безопасности баз данных; – 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; – методы контроля доступа, включая создание ролей и групп пользователей, управление правами доступа и аудит доступа к данным; – методы обнаружения и предотвращения атак, включая защиту от SQL-инъекций, DoS/DDoS-атак и других угроз безопасности; – методы мониторинга и анализа журналов событий для обнаружения угроз безопасности и анализа производительности базы данных; – методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование; – методы создания и управления бэкапами и резервными копиями данных, включая использование инкрементальных и дифференциальных бэкапов; – методы обеспечения безопасности базы данных при использовании облачных сервисов, включая защиту от утечки данных и управление доступом к облачным ресурсам; – законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.
ПК.3.1	<ul style="list-style-type: none"> – проводить сбор и анализ исходных данных для разработки проектной документации на информационную систему; 	<ul style="list-style-type: none"> – основные принципы и методы сбора и анализа исходных данных для разработки проектной документации на информационную

	<ul style="list-style-type: none"> – определять требования и функциональность информационной системы на основе собранных данных; – организовывать и управлять процессом сбора исходных данных для разработки проектной документации; – проводить анкетирование; – проводить интервьюирование 	<ul style="list-style-type: none"> систему; – возможности типовой ИС; – предметную область автоматизации; – инструменты и методы выявления требований; – 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; – устройство и функционирование современных ИС; – современные стандарты информационного взаимодействия систем; – программные средства и платформы инфраструктуры информационных технологий организаций; – системы классификации и кодирования информации, в том числе присвоение кодов документам и элементам справочников; – отраслевую нормативную техническую документацию; – источники информации, необходимой для профессиональной деятельности; – современный отечественный и зарубежный опыт в профессиональной деятельности; – основы бухгалтерского учета и отчетности организаций; – основы налогового законодательства Российской Федерации;
--	--	--

		<ul style="list-style-type: none"> – культуру речи; – правила деловой переписки –
ПК.3.2	<ul style="list-style-type: none"> – выбирать оптимальные технологии для реализации проекта; – разрабатывать планы проекта и управлять процессом разработки; – документировать проектную документацию в соответствии со стандартами и нормативными документами; – оценивать риски и принимать меры по их управлению 	<ul style="list-style-type: none"> – методологию разработки информационных систем; – принципы и методы анализа требований заказчика; – методы проектирования информационных систем и их компонентов; – принципы и методы выбора технологий для реализации проекта; – методы оценки рисков и управления проектом; – методы документирования проектной документации; – стандарты и нормативные документов в области разработки информационных систем; – принципы и методы обеспечения безопасности информационных систем; – принципы и методы управления изменениями в информационных
ПК.3.3	<ul style="list-style-type: none"> – анализировать требований безопасности информационных систем; – разрабатывать и реализовывать подсистемы безопасности информационных систем; – тестировать и проводить отладку подсистем безопасности информационных систем 	<ul style="list-style-type: none"> – принципы безопасности информационных систем; – современные методы и технологии в области безопасности информационных систем; – законодательных и нормативных актов в области безопасности информационных систем
ПК.3.5	<ul style="list-style-type: none"> – работать в команде над интеграцией модулей в информационную систему; – выполнять интеграцию программный модулей в программный продукт; – кодировать на языках программирования; – находить и анализировать ключевые понятия и термины в сторонней документации для интеграции, а также разбираться в их контексте и использовании в 	<ul style="list-style-type: none"> – принципы интеграции информационной системы с другими системами; – современные технологии и инструменты для разработки интеграции информационной системы; – принципы тестирования и отладки интеграции информационной системы; – форматы обмена данных; – интерфейсы обмена данных

	рамках проекта.	
ПК.3.7	<ul style="list-style-type: none"> – собирать и анализировать информацию о системе; – описывать процедуры установки и настройки системы; – описывать основные функции и возможности системы; – описывать процедуры обслуживания и регулярного обновления системы – разрабатывать руководство пользователя 	<ul style="list-style-type: none"> – принципы работы информационных систем; – процедуры установки и настройки системы; – типы, виды и содержание документации на информационные системы в соответствии с ISO и ГОСТ на каждом этапе жизненного цикла информационных систем

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	<i>Количество часов</i>
Максимальная учебная нагрузка (всего)	34
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
практические занятия	8
теоретические занятия	24
Самостоятельная работа обучающегося	2
Промежуточная аттестация в форме других форм контроля	

2.2. Тематический план и содержание предмета

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий, курсовой проект (работа)	Объем часов	Формируемые компетенции
1	2	3	4
Раздел 1. Основы работы с информацией		20	
Тема 1.1. Информационная культура и цифровая гигиена	Содержание учебного материала	4	
	Основы информационной среды: что такое информация и зачем ей управлять. Информационная перегрузка: стратегии фильтрации. Цифровая гигиена и личная инфосреда.	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
	Критическое мышление и проверка информации: Надёжные и ненадёжные источники: критерии оценки. Введение в фактчекинг: уровни лжи и методы опровержения	2	
	В том числе практических занятий	2	
	1. Деконструкция манипулятивных текстов: разбор новостного поста и выявление искажений	2	
Тема 1.2. Организация, хранение и использование данных	Содержание учебного материала	4	
	Основы организации и хранения информации: Структура файлов и папок логика и автоматизация. Организация хранилищ в облаке и на локальных устройствах. Типы данных и носителей: от архива до дата-центра.	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
	Систематизация и описание данных. Принципы каталогизации и индексирования. Метаданные: зачем нужны и как правильно задавать. Основы документирования информации	2	
	В том числе практических занятий	2	
	2. Создание структурированной базы данных (например, каталог медиафайлов с метаданными и фильтрами).	2	
Тема 1.3. Правовые и этические аспекты информационной работы	Содержание учебного материала	6	
	Правовые рамки и нормативное регулирование. Авторское право: что можно использовать, а что — нет. Свободные лицензии: Creative Commons и публичное достояние. Закон о персональных данных и GDPR: базовое знание. Работа с конфиденциальной информацией: что нельзя разглашать.	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
	Проверка достоверности и борьба с дезинформацией: Проверка источников: как удостовериться в достоверности. Инструменты фактчекинга: Snopes, Factcheck.org, Provereno. Признаки фейков: от фотофальсификации до deepfake	2	

	Академическая и профессиональная этика: Цитирование и плагиат: правила, инструменты, ловушки. Этическое курирование контента: как не навредить. Профессиональная репутация и след в интернете	2	
	В том числе практических занятий	2	
	3. Фактчекинг-кейс: разоблачение ложной информации (с применением онлайн-инструментов и логики проверки). Подготовка материала с соблюдением авторских прав: оформление сносок, атрибуции, выбор лицензии.	2	
Раздел 2. Основы информационной безопасности		14	
Тема 2.1. Введение в информационную безопасность	Содержание учебного материала	2	
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
Тема 2.2. Управление безопасностью информации	Содержание учебного материала	2	
	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, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
Тема 2.3. Криптография	Содержание учебного материала	4	
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
	В том числе практических занятий	2	
	4. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	
Тема 2.4. Защита сетевой инфраструктуры	Содержание учебного материала	2	
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4
Тема 2.5. Безопасность приложений	Содержание учебного материала	2	
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.5, ПК 3.7
Промежуточная аттестация в форме дифференцированного зачета			

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие лаборатории «Основы информационной безопасности». Оборудование лаборатории Информационных технологий:

- рабочее место преподавателя с персональным компьютером;
- посадочные места обучающихся (по количеству обучающихся);
- посадочные места обучающихся с персональными компьютерами;
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением;
- мультимедиапроектор;
- интерактивная доска.

Раздаточный материал: тестовые задания, индивидуальные карточки, дидактический материал по разделам и темам программы

3.2. Учебно-методическое обеспечение

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> (дата обращения: 16.11.2024).

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> (дата обращения: 16.11.2024).

3. 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> (дата обращения: 16.11.2024)

4. 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> (дата обращения: 16.11.2024)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоенности компетенций	Методы оценки
<p>Знает:</p> <ul style="list-style-type: none"> - 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 	<p>Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить;</p> <p>Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте;</p> <p>Знает алгоритмы выполнения работ в профессиональной и смежных областях;</p> <p>Знает методы работы в профессиональной и смежных сферах;</p> <p>Знает структуру плана для решения задач;</p> <p>Может произвести оценку результатов решения задач профессиональной деятельности</p> <p>Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности;</p> <p>Знает приемы структурирования информации;</p> <p>Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;</p> <p>Может применять современные средства и устройства информатизации и программное обеспечение</p>	<p>Экспертное наблюдение выполнения практических работ и видов работ по практике</p> <p>Диагностика (тестирование, контрольные работы)</p>

<p>информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;</p> <ul style="list-style-type: none"> - 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 	<p>в профессиональной деятельности в том числе с использованием цифровых средств;</p> <p>Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности;</p> <p>Знает принципы безопасности хранения данных;</p> <p>Владеет методами защиты баз данных от внешних угроз</p> <p>Знает принципы криптографии и методов шифрования данных;</p> <p>Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.;</p> <p>Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных</p> <p>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;</p> <p>Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;</p> <p>Знает современный отечественный и зарубежный опыт в</p>	
---	---	--

<p>профессиональной деятельности;</p> <ul style="list-style-type: none"> - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; <p>- современные методы и технологии в области безопасности информационных систем;</p> <ul style="list-style-type: none"> - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; <p>- принципы криптографии и шифрования данных;</p> <p>- стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;</p> <ul style="list-style-type: none"> - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; <p>- стандартные криптографические алгоритмы для шифрования данных;</p> <ul style="list-style-type: none"> - принципы обеспечения безопасности передачи 	<p>профессиональной деятельности;</p> <p>Владеет принципами и методами обеспечения безопасности информационных систем;</p> <p>Знает принципы безопасности информационных систем;</p> <p>Владеет современными методами и технологиями в области безопасности информационных систем;</p> <p>Знает законодательные и нормативные акты в области безопасности информационных систем;</p> <p>Знает источники угроз информационной безопасности и меры по их предотвращению;</p> <p>Имеет представление об основных угрозах безопасности мобильных приложений;</p> <p>Ориентируется в принципах криптографии и шифрования данных;</p> <p>Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;</p> <p>Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;</p> <p>Владеет основными принципами безопасности информации и методов ее защиты;</p> <p>Знает стандартные криптографические алгоритмы для шифрования данных;</p> <p>Имеет представление о</p>	
---	---	--

<p>данных по сети;</p> <ul style="list-style-type: none"> - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. <p>Умеет:</p> <ul style="list-style-type: none"> -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 	<p>принципах обеспечения безопасности передачи данных по сети;</p> <p>Знает основы безопасности приложений и инфраструктуры;</p> <p>Знает методы анализа на уязвимости и мониторинга безопасности;</p> <p>Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;</p> <p>Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения;</p> <p>Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</p> <p>Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте;</p> <p>Анализирует задачу и/или проблему и может выделить её составные части;</p> <p>Умеет определять этапы решения задачи;</p> <p>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или</p>	
--	--	--

<p>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;</p> <p>- 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; - понимать тексты на</p>	<p>проблемы; Составляет план действия;</p> <p>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);</p> <p>Умеет определять задачи для поиска информации; Умеет определять необходимые источники информации; Планирует процесс поиска;</p> <p>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;</p> <p>Может использовать современное программное обеспечение; Может использовать различные цифровые средства для решения профессиональных задач; Понимает тексты на базовые</p>	
--	--	--

<p>базовые профессиональные темы;</p> <ul style="list-style-type: none">- шифрование данных и обеспечивает их конфиденциальность;- анализировать требования безопасности информационных систем;- разрабатывать и реализовывать меры безопасности;- реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	<p>профессиональные темы;</p> <p>Умеет шифровать данные и обеспечивать их конфиденциальность;</p> <p>Умеет анализировать требования безопасности информационных систем;</p> <p>Может разрабатывать и реализовывать меры безопасности;</p> <p>Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.</p>	
--	---	--