Частное образовательное учреждение высшего образования
«Международный Институт Дизайна и Сервиса»
(ЧОУВО МИДиС)

Кафедра математики и информатики

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОПЦ.03 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 09.02.11 Разработка и управление программным обеспечением
Направленность (профиль): Разработка веб и мобильных приложений
Квалификация выпускника: Программист
Уровень базового образования обучающегося: Среднее общее образование
Форма обучения: Очная
Год набора: 2026

Челябинск 2026

Рабочая программа учебной дисциплины ОПЦ.02 Основы информационной безопасности разработана на основе требований федерального государственного образовательного стандарта среднего общего образования (приказ Министерства образования и науки РФ от 18 мая 2023 г. № 371) с учетом требований ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Министерства образования и науки РФ от 24 февраля 2025 г. № 138, профиля получаемого профессионального образования и примерной программы учебной дисциплины ОПЦ.02 Основы информационной безопасности

Автор-составитель: Прокопов И.И

Рабочая программа рассмотрена и одобрена на заседании кафедры математики и информатики. Протокол № 10 от 25.05.2026 г.

Заведующий кафедрой математики и информатики С.А. Кондаков

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОПЦ.02 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре основной профессиональной образовательной программы (образовательной программы)

Дисциплина является обязательной частью общепрофессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Особое значение дисциплина имеет при формировании и развитии ОК 01,02, ПК-1.5.

1.2. Цель и планируемые результатам освоения дисциплины:

Цель дисциплины «Основы информационной безопасности» формирование у студентов 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.

В рамках программы дисциплины обучающимися осваиваются следующие умения и знания:

Перечень формируемых компетенций

Код ОК	Умения	Знания	Навыки
ОК.01	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)	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	
ОК.02	определять задачи для поиска информации; определять необходимые источники информации;	номенклатура информационных источников, применяемых в профессиональной	

	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	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.	
ПК 1.5	шифровать данные и обеспечивать их конфиденциальность	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.	− использования стандартных методов защиты объектов базы данных; − разработки и внедрения систем защиты баз данных от несанкционированного доступа; − разработки и внедрения систем резервного копирования и восстановления баз данных; аудита безопасности баз данных

Личностные результаты реализации программы воспитания

Личностные результаты реализации рабочей программы воспитания *(дескрипторы)*	**Код личностных результатов реализации рабочей программы воспитания**
Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях;	**ЛР 6**
Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп.	**ЛР 8**

Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства;	
Пользоваться профессиональной документацией на государственном и иностранном языках. (в ред. Приказа Минпросвещения России от 17.12.2020 N 747)	**ЛР 16**
Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения (в ред. Приказа Минпросвещения России от 17.12.2020 N 747)	**ЛР 17**
Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. (в ред. Приказа Минпросвещения России от 17.12.2020 N 747)	**ЛР 18**
Активно применять полученные знания на практике.	**ЛР 22**
Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	**ЛР 23**
Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	**ЛР 24**
Проявлять доброжелательность к окружающим, деликатность, чувство такта и готовность оказать услугу каждому кто в ней нуждается.	**ЛР 25**

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**	**Разделение по семестрам**
		3 семестр
Объем образовательной программы учебной дисциплины	**32**	32
в т.ч. в форме практической подготовки	**32**	32
в том числе:		
теоретическое обучение	**12**	12
практические занятия	**20**	20
Самостоятельная работа	-	-
Промежуточная аттестация	-	зачет с оценкой

2.2 Тематический план и содержание учебной дисциплины ОПЦ.02 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч. / в том числе в форме практической подготовки, акад. ч.	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
1	2	3	4
	3 семестр		
Тема 1. Введение в информационную безопасность	**Содержание учебного материала**	**1**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности		
Тема 2. Управление безопасностью информации	**Содержание учебного материала**	**1**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
Тема 3. Криптография	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	В том числе практических занятий и лабораторных работ	**4**	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
Тема 4. Защита сетевой инфраструктуры	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов		
	В том числе практических занятий и лабораторных работ	**2**	
	Организация защиты от атак Организация работы VPN и межсетевого экрана		
Тема 5.	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5

Безопасность приложений	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		ЛР 6,8,16-18,22-25
	В том числе практических занятий и лабораторных работ	**2**	
	Тестирование на проникновение и анализ уязвимостей.		
Тема 6. Защита данных	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	В том числе практических занятий и лабораторных работ	**4**	
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным		
Тема 7. Безопасность облачных технологий	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	В том числе практических занятий и лабораторных работ	**2**	
	Изучение модели облачных услуг и их безопасности		
Тема 8. Инциденты безопасности	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	В том числе практических занятий и лабораторных работ	**2**	
	Работа с инцидентами.		
Тема 9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**	**4**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	В том числе практических занятий и лабораторных работ	**4**	
	Разработка политики информационной безопасности		
Тема 10. Будущее информационной безопасности	**Содержание учебного материала**	**2**	ОК 01, ОК 02, ПК 1.5 ЛР 6,8,16-18,22-25
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
	Промежуточная аттестация	Зачет с оценкой	

Всего:	**32**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация общепрофессиональной учебной дисциплины ОПЦ.03 Основы информационной безопасности предусматривает наличия учебного кабинета математических дисциплин.

Помещение учебного кабинета удовлетворяет требованиям Санитарно-эпидемиологических правил и нормативов (СанПин 2.4.3648-20).

№ п/п	Наименование оборудованных учебных аудиторий для практических занятий, лабораторий, мастерских	Перечень материального оснащения, оборудования и технических средств обучения
1.	**Лаборатория информатики и информационных технологий № 245** **№ 245 Лаборатория информационных ресурсов № 245**	**Лаборатория информатики и информационных технологий. Лаборатория информационных ресурсов № 245** (Лаборатория для проведения занятий всех видов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации) *Материальное оснащение, компьютерное и интерактивное оборудование:* Компьютер Проектор Экран для проектора Компьютерный стол Стулья Стол преподавателя Стул преподавателя. Доска магнитно-маркерная Картины **Условия для лиц с ОВЗ:** Клавиатура с нанесением шрифта Брайля Компьютер с программным обеспечением для лиц с ОВЗ Расширенный дверной проем Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду МИДиС, выходом в информационно-коммуникационную сеть «Интернет». *Лицензионное и свободно распространяемое программное обеспечение* 1С: Предприятие. Комплект для высших и средних учебных заведений (1С – 8985755) Битрикс 24 Яндекс браузер Mozilla Firefox Adobe Reader Microsoft™ Office® МойОфис Антивирус «Касперский» (Kaspersky Endpoint Security**)** VS Code / JetBrains Edu Python + scikit-learn, PyTorch Unity (Personal/Edu) Blender Git + GitHub/GitLab Jira / YouTrack (Edu) Figma (Edu) PostgreSQL / MySQL Docker Desktop (Edu) «Гарант аэро» КонсультантПлюс
2.	**Библиотека. Читальный зал № 122**	**Библиотека. Читальный зал с выходом в Интернет № 122** Автоматизированные рабочие места библиотекарей Автоматизированные рабочие места для читателей Принтер

		Сканер Стеллажи для книг Кафедра Выставочный стеллаж Каталожный шкаф Посадочные места (столы и стулья для самостоятельной работы) Стенд информационный **Условия для лиц с ОВЗ:** Автоматизированное рабочее место для лиц с ОВЗ Линза Френеля Специальная парта для лиц с нарушениями опорно-двигательного аппарата Клавиатура с нанесением шрифта Брайля Компьютер с программным обеспечением для лиц с ОВЗ Световые маяки на дверях библиотеки Тактильные указатели направления движения Тактильные указатели выхода из помещения Контрастное выделение проемов входов и выходов из помещения Табличка с наименованием библиотеки, выполненная шрифтом Брайля Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду МИДиС, выходом в информационно-коммуникационную сеть «Интернет». *Лицензионное и свободно распространяемое программное обеспечение* 1С: Предприятие. Комплект для высших и средних учебных заведений (1С – 8985755) Битрикс 24 Яндекс браузер Mozilla Firefox Adobe Reader Microsoft™ Office® МойОфис Антивирус «Касперский» (Kaspersky Endpoint Security) «Гарант аэро» КонсультантПлюс

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные и электронных издания

Печатные издания

1.Бубнов, А.А. Основы информационной безопасности: учеб. пособие для спо / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. - 3-е изд. - М.: Академия, 2023. - 256 с.

Электронные издания (электронные ресурсы)

1. Внуков, А.А. Основы информационной безопасности: защита информации: учебное пособие для спо / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Юрайт, 2026. — 161 с. —Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458 (дата обращения: 20.05.2026).

2. Зенков, А.В. Информационная безопасность и защита информации: учебник / А.В. Зенков. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2026. — 107 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741 (дата обращения: 20.05.2026).

3. Казарин, О.В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для спо / О.В. Казарин, И.Б. Шубинский. — 2-е изд. — Москва: Юрайт, 2026. — 352 с. —Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457 (дата обращения: 20.05.2026).

4. Организационное и правовое обеспечение информационной безопасности: учебник для спо / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2026. —

357 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584372 (дата обращения: 20.05.2026).
5. Щербак, А.В. Информационная безопасность: учебник для спо / А.В. Щербак. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2026. — 252 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374 (дата обращения: 20.05.2026).

Дополнительные источники *(при необходимости)*

1. Богатырев, В.А. Информационные системы и технологии. Теория надежности: учебное пособие / В.А. Богатырев. — 2-е изд. — Москва: Юрайт, 2026. — 366 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590557 (дата обращения: 20.05.2026).
2. Внуков, А.А. Защита информации: учебник / А.А. Внуков. — 3-е изд., перераб. и доп. — Москва: Юрайт, 2026. — 161 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584050 (дата обращения: 20.05.2026).
3. Щеглов, А.Ю. Защита информации: основы теории: учебник / А.Ю. Щеглов, К.А. Щеглов. — Москва: Юрайт, 2026. — 349 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583858 (дата обращения: 20.05.2026).

3.2.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения учебной дисциплины

Для выполнения заданий, предусмотренных рабочей программой, используются рекомендованные Интернет-сайты, ЭБС.

Электронные образовательные ресурсы

1. Образовательная платформа «ЮРАЙТ »http://www.urait.ru
2. Справочно-правовая система "ГАРАНТ. "https://www.garant.ru
3. Некоммерческая интернет-версия системы «КонсультантПлюс http://base.consultant.ru/cons/cgi/online.cgi?req=home
4. Правовые ресурсы в сети интернет http://www.nlr.ru/lawcenter/ires/
5. Справочная система «Консультант» http://www.consultant.ru
6. eLIBRARY.RU: Научная электронная библиотека http://elibrary.ru
7. Министерство обороны РФ http://mil.ru/index.htm

Современные профессиональные базы данных и информационно-справочные системы

1. База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru
2. StackOverflow — это самая большая база вопросов и ответов по программированию Статистика и отчеты Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации https://digital.gov.ru/ru/activity/statistic/#section-informatsionno-kommunikatsionnyie-tehnologii-v-tsifrah
3. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки https://github.com
4. ХАБР: База данных для IT-специалистов: статьи и новости на ITT-тематику https://habr.com/ru
5. Science Direct (содержит более 1500 журналов издательства Elsevier) https://www.sciencedirect.com/
6. Megabook – Мегаэнциклопедия Кирилла и Мефодия http://megabook.ru
7. Online словарь и тезаурус Cambridge Dictionary https://dictionary.cambridge.org/ru/
8. База данных Всероссийского центра изучения общественного мнения (ВЦИОМ) https://wciom.ru/
9. StackOverflow — это самая большая база вопросов и ответов по программированию stackoverflow.com
10. Киберфорум cyberforum.ru

11. Сайт по веб-разработке для новичков: HTML + CSS + JavaScript. doka.guide
12. Хабр –разработка https://habr.com/ru/flows/develop/articles/

Сведения об электронно-библиотечной системе

№ п/п	Основные сведения об электронно-библиотечной системе	Краткая характеристика
1	Наименование электронно-библиотечной системы, представляющей возможность круглосуточного дистанционного индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет, адрес в сети Интернет	Образовательная платформа «Юрайт»: https://urait.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения	**Критерии оценки**	**Формы и методы оценки**
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	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	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием 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;	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 использованием 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	

- 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 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 на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз	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; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, 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 на уязвимости и мониторинга безопасности;	

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. ***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;	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. 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	

- 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 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.	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; 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.	