

Приложение 2.25
к ОПОП-П по специальности
09.02.11 Разработка и управление программным обеспечением

Рабочая программа дисциплины
«ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

2026 г.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	3
1.1. Цель и место дисциплины в структуре образовательной программы.....	3
1.2. Планируемые результаты освоения дисциплины	3
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	5
2.1. Трудоёмкость освоения дисциплины	5
2.2. Содержание дисциплины.....	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ	15
3.1. Материально-техническое обеспечение.....	15
3.2. Учебно-методическое обеспечение	15
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	16

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Цель и место дисциплины в структуре образовательной программы

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

1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать
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; 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 1.1	-	принципы безопасности хранения данных
ПК 1.4	-	методы защиты баз данных от внешних угроз

Код ОК, ПК	Уметь	Знать
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.
ПК 3.1	-	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности
ПК 3.1	-	современный отечественный и зарубежный опыт в профессиональной деятельности
ПК 3.2	-	принципы и методы обеспечения безопасности информационных систем
ПК 3.3	анализ требований безопасности информационных систем	принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем
ПК 3.5	-	источники угроз информационной безопасности и меры по их предотвращению
ПК 3.7	разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	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

<i>Код ОК, ПК</i>	Уметь	Знать
		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

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоёмкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки
Учебные занятия	36	22
Лекции	26	12
Практические занятия	10	10
Самостоятельная работа	10	
Промежуточная аттестация в форме зачета	-	
Всего	46	22

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационно й безопасности		46	22	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.1. Введение в информационну ю безопасность	Содержание	2	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.1. Введение в информационну ю безопасность	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 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.2. Управление безопасностью информации	Содержание	4	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.7
Тема 1.2. Управление безопасностью информации	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.).	4	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.3. Криптография	Содержание	4	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.3. Криптография	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	4	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.3. Криптография	В том числе практических занятий	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.3. Криптография	Практическое занятие №1. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.4. Защита сетевой инфраструктуры	Содержание	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.4. Защита сетевой инфраструктуры	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.). Использование VPN и межсетевых экранов.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.4. Защита сетевой инфраструктуры	В том числе практических занятий	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.4. Защита сетевой инфраструктуры	Практическое занятие №2. Организация защиты от атак. Организация работы VPN и межсетевого экрана.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.5. Безопасность приложений	Содержание	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.5. Безопасность приложений	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.6. Защита данных	Содержание	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.6. Защита данных	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.6. Защита данных	В том числе практических занятий	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.6. Защита данных	Практическое занятие №3. Тестирование на проникновение и анализ уязвимостей. Выполнение резервного копирования и восстановления данных. Управление доступом к данным.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.7.	Содержание	2	-	ОК 01, ОК 02,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
Безопасность облачных технологий				ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.7. Безопасность облачных технологий	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность.	2	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.8. Инциденты безопасности	Содержание	4	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.8. Инциденты безопасности	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж.	4	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
	OSINT. Форензика.			
Тема 1.8. Инциденты безопасности	В том числе практических занятий	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.8. Инциденты безопасности	Практическое занятие №4. Изучение модели облачных услуг и их безопасности. Работа с инцидентами.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.9. Социальная инженерия и человеческий фактор	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.7
Тема 1.9. Социальная инженерия и человеческий фактор	В том числе практических занятий	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.9. Социальная инженерия и человеческий фактор	Практическое занятие №5. Разработка политики информационной безопасности.	2	2	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.10. Будущее информационно й безопасности	Содержание	2	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Тема 1.10. Будущее информационно й безопасности	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.	2	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5,

Наименование разделов и тем	Содержание учебного материала, практических занятий,	Объём в часах	В том числе в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
				ПК 3.7
Самостоятельная работа обучающихся	Проработка учебного материала по темам 1.1–1.10; закрепление основных понятий информационной безопасности, анализ требований политики информационной безопасности, примеров применения криптографических алгоритмов, схем защиты сетевой инфраструктуры, типовых уязвимостей веб-приложений, рисков облачных сред, алгоритмов реагирования на инциденты и перспективных технологий информационной безопасности.	10	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Промежуточная аттестация (зачет)	Зачет.	-	-	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
Всего		46	22	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации имеет печатные и электронные образовательные и информационные ресурсы для использования в образовательном процессе.

3.2.1. Основные печатные и/или электронные издания

1. Щербак, А. В. Информационная безопасность : учебное пособие / А. В. Щербак. — Москва : Издательство Юрайт. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/informacionnaya-bezopasnost-567521>.
2. Нестеров, С. А. Информационная безопасность : учебное пособие / С. А. Нестеров. — Москва : Издательство Юрайт. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/informacionnaya-bezopasnost-442312>.
3. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Москва : Издательство Юрайт. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/informacionnaya-bezopasnost-567672>.
4. Информационная безопасность и защита информации : учебное пособие. — Москва : Издательство Юрайт. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-544290>.
5. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2023. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/141624>.
6. Основы информационной безопасности : учебное пособие. — Саратов : Профобразование. — ISBN 978-5-4488-2237-7. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/142816>.
7. Основы информационной безопасности : учебное пособие. — Саратов : Профобразование. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/91640>.
8. Основы информационной безопасности : учебное пособие. — Саратов : Профобразование. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/142285>.
9. Основы информационной безопасности и защита информации : учебное пособие. — Саратов : Профобразование. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование : [сайт]. — URL: <https://profspo.ru/books/128718>.
10. Нечаев, А. М. Компьютерные сети : учебник для среднего профессионального образования / А. М. Нечаев. — Москва : Издательство Юрайт. — (Профессиональное образование). — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/kompyuternye-seti-572240>.

3.2.2. Дополнительные источники

1. Нечаев, А. М. Компьютерные и телекоммуникационные сети : учебник для среднего профессионального образования / А. М. Нечаев. — Москва : Издательство Юрайт. — (Профессиональное образование). — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/bcode/572242>.
2. Компьютерные сети и системы связи. Вводный курс : учебное пособие. — Москва : Издательство Юрайт. — ISBN 978-5-534-21489-5. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/bcode/572633>.
3. Информационные технологии : учебник для среднего профессионального образования / В. В. Трофимов, О. П. Ильина, В. И. Кияев, Е. В. Трофимова ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2025. — 546 с. — (Профессиональное образование). — ISBN 978-5-534-18341-2. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/bcode/568882>.
4. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — Москва : Издательство Юрайт. — (Профессиональное образование). — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: <https://urait.ru/book/informatika-i-informacionnye-tehnologii-557964>.
5. Мухин, О. И. Основы искусственного интеллекта : 10-11-е классы : учебное пособие для технологического профиля / О. И. Мухин. - Москва : Просвещение, 2026. - 369 с. - (Профильная школа). - ISBN 978-5-09-130025-3. - Текст : электронный // ЭБС Znanium : [сайт]. - URL: <https://znanium.ru/catalog/product/2233316>.
6. Операционные системы : учебное пособие. — Саратов : Профобразование. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО ПРОФобразование : [сайт]. — URL: <https://profspo.ru/books/115697>.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости компетенций	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 информации; Знает формат оформления результатов поиска информации, современные средства и устройства информатизации; Может применять современные средства и устройства информатизации и	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

Результаты обучения	Показатели освоенности компетенций	Методы оценки
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; - 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,	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 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;	

Результаты обучения	Показатели освоённости компетенций	Методы оценки
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 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 ресурсы	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; 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 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;	

Результаты обучения	Показатели освоения компетенций	Методы оценки
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; - 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 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.	