Министерство образования и науки Самарской области

АССОЦИАЦИЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ «ИНСТИТУТ НАПРАВО.РУ»



УТВЕРЖДАЮ
Приказ директора
ИНСТИТУТ НАПРАВО.РУ
от 08.06.2026 г № 022/с

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«общепрофессиональный цикл»
образовательной программы подготовки специалистов среднего звена
09.02.11 Разработка и управление программным обеспечением

Тольятти, 2026

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 9

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ..... 14

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ..... 17

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.04 ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.05 Основы информационной безопасности является обязательной частью общепрофессионального цикла программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Учебная дисциплина ОП.05 Основы информационной безопасности обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2 Цель и планируемые результаты освоения дисциплины

В результате изучения дисциплины обучающимися осваиваются элементы компетенций:

Код	Наименование ОК, ПК
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
ПК 1.1	Проектировать базы данных
ПК 1.4	Администрировать базы данных
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации.
ПК 3.2	Собирать исходные данные для разработки проектной документации на информационную систему.

Код	Наименование ОК, ПК
ПК 3.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием
ПК 3.5	Интегрировать информационную систему с существующими информационными системами заказчика
ПК 3.7	Разрабатывать техническую документацию на эксплуатацию информационной системы.

Базовая часть

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Код умения	Уметь	Код знания	Знать	Код навыка	Владеть навыками
ОК 01	У 1	выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы	31.	структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях		–
ОК 02	У 2	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации	32.	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации		–
ОК 09	У 3	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы	33.	правила построения простых и сложных предложений на профессиональные темы		–
ПК 1.1			34.	принципы безопасности хранения данных		
ПК 1.4			35.	методы защиты баз данных от внешних угроз		
ПК 1.5	У 4	шифровать данные и обеспечивать их конфиденциальность	36. 37. 38. 39.	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.		

Код ОК, ПК	Код умения	Уметь	Код знания	Знать	Код навыка	Владеть навыками
ПК 3.1			310. 311. 312.	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности современный отечественный и зарубежный опыт в профессиональной деятельности		
ПК 3.2			313.	принципы и методы обеспечения безопасности информационных систем		
ПК 3.3	У 5	анализ требований безопасности информационных систем	314. 315. 316.	принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем	Н1.	применение современных методов и технологий в области безопасности информационных систем
ПК 3.5			317.	источники угроз информационной безопасности и меры по их предотвращению		
ПК 3.7	У 6 У 7	разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	318. 319.	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных	Н2. Н3.	использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные применение механизмов хеширования для защиты паролей пользователей от

Код ОК, ПК	Код умения	Уметь	Код знания	Знать	Код навыка	Владеть навыками
						несанкционированного доступа
			320.	стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect	Н4.	обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS
			321.	законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA	Н5.	соблюдение законодательства и регуляций в области защиты данных
			322.	основные принципы безопасности информации и методов ее защиты		
			323.	стандартные криптографические алгоритмы для шифрования данных		
			324.	принципы обеспечения безопасности передачи данных по сети		
			325.	основы безопасности приложений и инфраструктуры		
			326.	методы анализа на уязвимости и мониторинга безопасности		
			327.	знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений		

Вариативная часть[1]

НЕ ПРЕДУСМОТРЕНО

[1] *Если имеется. В случае отсутствии вариативной части, пишется «НЕ ПРЕДУСМОТРЕНО»*

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы учебной дисциплины	36
В т.ч. в форме практической подготовки	23
Объем образовательной программы во взаимодействии с преподавателем	36
в том числе:	
теоретическое обучение	11
лабораторные занятия	*не предусмотрено*
практические занятия	23
курсовая работа (проект)	*не предусмотрено*
контрольная работа	*не предусмотрено*
Самостоятельная работа	*не предусмотрено*
Промежуточная аттестация	
в форме комплексного дифференциального зачета	*2*

2.2. Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов/в форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы,
Раздел 1 Основы информационной безопасности		**36**	
Тема 1.1. Введение в информационную безопасность	**Содержание учебного материала**	**1**	
	1. Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	1	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
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	*не предусмотрено*	
	Контрольная работа	*не предусмотрено*	
	Самостоятельная работа	*не предусмотрено*	
Тема 1.2. Управление безопасностью информации	**Содержание учебного материала**	**1**	
	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.)	1	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
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	*не предусмотрено*	
	Самостоятельная работа обучающихся	*не предусмотрено*	
Тема 1.3. Криптография	**Содержание учебного материала**	**2**	
	1. 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 3.1, ПК 3.2, ПК 3.3, ПК 3.5. ПК 3.7
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	**4**	
	1. Работа с симметричными и асимметричными алгоритмами.	*2*	ОК 01, ОК 02, ОК 09, ПК 1.1, ПК 1.4, ПК 1.5, ПК
	2. Хэширование и создание цифровой подписи сообщения.	*2*	

	Контрольная работа	*не предусмотрено*	3.1, ПК 3.2, ПК 3.3, ПК 3.5. ПК 3.7
	Самостоятельная работа обучающихся	*не предусмотрено*	
Тема 1.4. Защита сетевой инфраструктуры	**Содержание учебного материала**	**1**	
	1. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.)	1	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
	2. Использование VPN и межсетевых экранов		
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	**4**	
	1. Организация защиты от атак	2	
	2. Организация работы VPN и межсетевого экрана	2	
	Контрольная работа	*не предусмотрено*	
	Самостоятельная работа обучающихся	*не предусмотрено*	
Тема 1.5. Безопасность приложений	**Содержание учебного материала**	**1**	
	1. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики.	1	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
	2. Тестирование на проникновение и анализ уязвимостей.		
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	**2**	
	1. Тестирование на проникновение и анализ уязвимостей.	2	
	Контрольная работа	*не предусмотрено*	
	Самостоятельная работа обучающихся	*не предусмотрено*	
Тема 1.6. Защита данных	**Содержание учебного материала**	**2**	
	1. Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных.	1	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
	2. Управление доступом к данным	1	
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	**4**	
	1. Выполнение резервного копирования и восстановления данных.	2	

	2.	Управление доступом к данным	2	
	Контрольная работа		*не предусмотрено*	
	Самостоятельная работа обучающихся		*не предусмотрено*	
Тема 1.7. Безопасность облачных технологий	**Содержание учебного материала**		**1**	
	1.	Особенности безопасности в облачных средах.	1	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
	2.	Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	Лабораторная работа		*не предусмотрено*	
	Практические занятия		**4**	
	1.	Изучение модели облачных услуг и их безопасности	4	
	Контрольная работа		*не предусмотрено*	
	Самостоятельная работа обучающихся		*не предусмотрено*	
Тема 1.8. Инциденты безопасности	**Содержание учебного материала**		**1**	
	1.	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента.	1	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
	2.	Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	Лабораторная работа		*не предусмотрено*	
	Практические занятия		**2**	
	1.	Работа с инцидентами.	2	
	Контрольная работа		*не предусмотрено*	
	Самостоятельная работа обучающихся		*не предусмотрено*	
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**		**1**	
	1.	Психология атак: социальная инженерия.	1	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
	2.	Обучение сотрудников информационной безопасности		
	Лабораторная работа		*не предусмотрено*	

	Практические занятия	**3**	
	1. Разработка политики информационной безопасности	3	
	Контрольная работа	*не предусмотрено*	
	Самостоятельная работа обучающихся	*не предусмотрено*	
Тема 1.10. Будущее информационной безопасности	**Содержание учебного материала**	**1**	
	1. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн).	1	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
	2. Этические аспекты информационной безопасности		
	Лабораторная работа	*не предусмотрено*	
	Практические занятия	*не предусмотрено*	
	Контрольная работа	*не предусмотрено*	
	Самостоятельная работа обучающихся	*не предусмотрено*	
Курсовой проект (работа) *(для специальности, если предусмотрено)*		*не предусмотрено*	
Промежуточная аттестация			
Комплексный дифференцированный зачет		**2**	
Всего:		**36**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная необходимым для реализации программы учебной дисциплины оборудованием, техническими средствами и мебелью.

№	Наименование	Тип
1.	Посадочные места по количеству обучающихся (столы, стулья)	Мебель
2.	Рабочее место преподавателя	Мебель
3.	Шкаф или полки для хранения учебной и методической литературы	Мебель
4.	Доска маркерная	Мебель
5.	ПК преподавателя (системный блок, монитор, клавиатура, мышь) ЦПУ: - Intel(R) Core(TM) i3-10100 - количество физических ядер - 4 - количество потоков - 8 Сетевой адаптер: - технология Ethernet - 10/100/1000 mbps ОЗУ: - 8 ГБ Графический адаптер: - NVIDIA GeForce GT730 ПЗУ:- SSD 256 ГБ	ТС
6.	ПК (системный блок, монитор, клавиатура, мышь) по количеству обучающихся ЦПУ: - Intel(R) Core(TM) i3-10100 - количество физических ядер - 4 - количество потоков - 8 Сетевой адаптер: - технология Ethernet - 10/100/1000 mbps ОЗУ: - 8 ГБ Графический адаптер: - NVIDIA GeForce GT730 ПЗУ:- SSD 256 ГБ	ТС
7.	Мультимедийный проектор	ТС
8.	Аудио- и видеооборудование	ТС
9.	Комплект учебно-методических материалов	УМК

Наименование лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Операционная система (РЕД ОС 8.0 или аналог)
2. Клиент для работы с API (Postman или аналог)
3. Программное обеспечение для записи экрана (OBS Studio или аналог)
4. Эмулятор выполняемой среды (Genymotion, VirtualBox, VMWare Workstation или аналог)
5. Набор средств разработки (Node.js или аналог)
6. ПО веб-браузер (Яндекс Браузер, Chromium, Google Chrome или аналоги)
7. ПО Системы контроля версий (Git, GitKraken или аналоги)
8. Текстовый редактор (Sublime Text, Visual Studio Code или аналоги)

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1. Основные печатные и 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 (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)

3.2.2. Дополнительные источники

1. Электронно-библиотечная система Znanium [Электронный ресурс]. – Режим доступа: https://znanium.com/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения	Показатели освоенности 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 поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной	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	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

Результаты обучения	Показатели освоенности компетенций	Методы оценки
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;	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 деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных	

Результаты обучения	Показатели освоенности компетенций	Методы оценки
- 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 безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения	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; 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;	

Результаты обучения	Показатели освоенности компетенций	Методы оценки
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; - оценивать практическую значимость результатов поиска; - оформлять результаты поиска, применять средства	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;	

Результаты обучения	Показатели освоенности компетенций	Методы оценки
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.	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.	

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата внесения изменения; № страницы с изменением; .	
БЫЛО	**СТАЛО**
Основание: Подпись лица внесшего изменения	