МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АСТРАХАНСКОЙ ОБЛАСТИ
Государственное бюджетное образовательное учреждение Астраханской области высшего образования
«Астраханский государственный архитектурно – строительный университет»
(ГБОУ АОВО «АГАСУ»)
КОЛЛЕДЖ СТРОИТЕЛЬСТВА И ЭКОНОМИКИА ГАСУ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

среднего профессионального образования

09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Квалификация- Специалист по технической эксплуатации
и сопровождению информационных систем

2026

ОДОБРЕНО	РЕКОМЕНДОВАНО	УТВЕРЖДЕНО
предметно-цикловой комиссией «Математические и естественно научные дисциплины»	методическим советом –КСиЭ АГАСУ	директор КСиЭ АГАСУ
Протокол № 12	Протокол № 9	
от «28» 04 2026 г.	от «30» 04 2026 г.	С.Н. Коннова
председатель предметно-цикловой комиссии		«30» 04 2026 г.
С.В. Рассказова		
«28» 04 2026 г.		

Составитель: /А.И. Михайлова/

Рабочая программа разработана на основе ФГОС СПО специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем

Согласовано:

Методист КСиЭ АГАСУ /Д.С. Захарова/

Заведующий библиотекой /Л.С Гаврилова/

Заместитель директора по ПР /Н.Р. Новикова/

Заместитель директора по УР /Е.О. Черемных/

Специалист ООСиМ СПО / К.П. Мордвинова /

Рецензент
ФГБОУ ВО «АГТУ» факультет СПО
преподаватель высшей
квалификационной категории /М.М. Халдузова/

Принято ООСиМ СПО:

Начальник ООСиМ СПО /А.П. Гельван

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.06 «Основы информационной безопасности» является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

Рабочая программа учебной дисциплины может быть использована при разработке программ дополнительного образования (повышения квалификации и переподготовки) работников информационных систем.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина входит в общепрофессиональный цикл и является общепрофессиональной дисциплиной.

1.3. Цели и задачи дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен **уметь**:

- распознавать задачу и/или проблему в профессиональном и/или социальном контексте;
- анализировать задачу и/или проблему и выделять её составные части;
- определять этапы решения задачи;
- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;
- составлять план действия;
- определять необходимые ресурсы;
- владеть актуальными методами работы в профессиональной и смежных сферах;

- реализовывать составленный план;
- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);
- определять задачи для поиска информации;
- определять необходимые источники информации;
- планировать процесс поиска;
- структурировать получаемую информацию; - выделять наиболее значимое в перечне информации;
- оценивать практическую значимость результатов поиска;
- оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач;
- использовать современное программное обеспечение;
- 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.

В результате освоения учебной дисциплины обучающийся должен **знать:**

- актуальный профессиональный и социальный контекст, в котором приходится работать и жить;
- основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
- алгоритмы выполнения работ в профессиональной и смежных областях;
- методы работы в профессиональной и смежных сферах;
- структуру плана для решения задач;

− порядок оценки результатов решения задач профессиональной деятельности

− номенклатуру информационных источников, применяемых в профессиональной деятельности;

− приемы структурирования информации;

− формат оформления результатов поиска информации, современные средства и устройства информатизации;

− порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с 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, 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.

Содержание дисциплины ориентировано на подготовку студентов к освоению профессиональных модулей ППССЗ по специальности 09.02.12 «Техническая эксплуатация и сопровождение информационных систем» и овладению профессиональными (ПК) компетенциями:

ПК 1.7. Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем.

ПК 2.5. Выполнять восстановление тестов после сбоев, повлекших за собой нарушение работы системы, в том числе автоматизированных тестов.

В процессе освоения дисциплины у студентов должны быть сформированы общие компетенции (ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

1.4. Количество часов на освоение рабочей программы учебной дисциплины

Объем ОП – 72 часа

В том числе с преподавателем 54 часа;

Самостоятельной работы обучающегося – 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объём часов**
Максимальная учебная нагрузка (всего)	**72**
Обязательная аудиторная учебная нагрузка (всего)	**54**
в том числе:	
Практические занятия	30
Лабораторная занятия	-
Самостоятельная работа	12
- завершение и оформление отчетов по лабораторным и практическим работам; - подготовка и оформление рефератов	
Итоговый контроль предусмотрен в форме экзамена по завершению курса	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объём часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы и управление информационной безопасностью		**16**	
Тема 1. Введение в информационную безопасность	**Содержание учебного материала**	***10***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7, ПК 2.5
	1. Основные понятия и определения (конфиденциальность, целостность, доступность.). История и развитие ИБ. Актуальные угрозы и риски.	2	
	2. История и развитие ИБ. Актуальные угрозы и риски. Модели угроз. Понятие и классификация инцидентов ИБ..	2	
	В том числе практических и лабораторных занятий Практическая работа №1. Основы информационной безопасности	2	
	Практическая работа №2. Анализ рисков информационной безопасности на основе построения модели информационных потоков.	2	
	Практическая работа №3. Анализ рисков на основе модели угроз и уязвимостей	2	
	Самостоятельная работа обучающегося Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов: 1. Современные нормативные правовые акты РФ, регламентирующие информационную безопасность страны. 2. Понятие информационной безопасности и ее составных частей в современных НПАРФ. 3. Понятия целостности, конфиденциальности, аутентичности и доступности информации в современных НПА РФ. 4.Понятия защищенности информационных ресурсов, информационных систем и информационных технологий в современных НПА РФ.	**3**	
Тема 1.2. Управление безопасностью информации	**Содержание учебного материала**	***4***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7, ПК 2.5
	1. Нормативно-правовое регулирование (ФЗ-152 и т.п.). Политики и процедуры безопасности. Оценка рисков и управление ими. Основы ИБ организации.	2	

	Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
	В том числе практических и лабораторных занятий Практическая работа №4. Анализ основных нормативно-правовых документов по защите информации и противодействию технической разведке	2	
	Самостоятельная работа обучающегося Разработать реферат-презентацию на заданную тему с использованием содержания требований, найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов: 1. Понятие правового обеспечения информационной безопасности. 2. Особенности информации как объекта права. 3. Государственная политика РФ в области правового обеспечения. 4. Уровни правового регулирования в сфере информационной безопасности. 5. Основные конституционные и правовые нормы в области информационной безопасности. 6. Понятия банковской, коммерческой и служебной тайны. 7. Наказания за преступления в сфере компьютерной информации. 8. Зарубежное законодательство в области информационной безопасности.	**3**	
Тема 1.3. Социальная инженерия и человеческий фактор	**Содержание учебного материала**	***2***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 2.5
	1. Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности.	2	
	В том числе практических и лабораторных занятий	**-**	
	Самостоятельная работа обучающегося Разработка памятки для сотрудников по распознаванию фишинговых писем	**2**	
Раздел 2. Технические средства защиты информации		**34**	
Тема 2.1. Криптография	**Содержание учебного материала**	***6***	ОК 02, ОК 04, ОК 09 ПК 2.5
	1. Основы криптографии: симметричные, а асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических и лабораторных занятий		
	Практическая работа №5. Работа с симметричными и асимметричными алгоритмами.	2	

	Практическая работа №6. Хэширование и создание цифровой подписи сообщения	2	
	Самостоятельная работа обучающегося:	-	
Тема 2.2 Защита сетевой инфраструктуры	**Содержание учебного материала**	***6***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 2.5
	1. Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов.	2	
	В том числе практических и лабораторных занятий		
	Практическая работа № 7. Организация работа VPN и межсетевого экрана.	2	
	Практическая работа №8. Разработка схемы сегментации для минимизации последствий атак.	2	
	Самостоятельная работа обучающегося	-	
Тема 2.3. Безопасность приложений и данных	**Содержание учебного материала**	***6***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7, ПК 2.5
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей	2	
	Тестирование на проникновение и анализ уязвимостей. Выполнение резервного копирования и восстановления данных.	2	
	В том числе практических и лабораторных занятий Практическая работа №9. Тестирование безопасности	2	
	Самостоятельная работа обучающегося: Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов: 1. Классификация компьютерных вирусов и вредоносных программ. 2. Файловые, загрузочные и сетевые вирусы. 3. Методы и средства борьбы с вирусами и вредоносными программами. 4. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения	**3**	
Тема 2.4. Защита данных	**Содержание учебного материала**	***8***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7, ПК 2.5
	1. Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным.	2	
	В том числе практических и лабораторных занятий		
	Практическая работа №10. Выполнение резервного копирования и восстановления данных.	2	
	Практическая работа №11. Защита ячеек, формул и файлов на примере Excel	2	

	Практическая работа №12. Управление доступом к данным.	2	
	Самостоятельная работа обучающегося	-	
Тема 2.5. Безопасность облачных технологий	**Содержание учебного материала**	***2***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности.	2	
	В том числе практических и лабораторных занятий		
	Самостоятельная работа обучающегося	-	
Тема 2.6 Инциденты безопасности	**Содержание учебного материала**	***6***	ОК 01, ОК 02, ОК 04, ОК 09 ПК 1.7, ПК 2.5
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента.	2	
	В том числе практических и лабораторных занятий		
	Практическая работа №13-14. Работа с инцидентами.	4	
	Самостоятельная работа обучающегося	-	
Раздел 3. Перспективы развития информационной безопасности		**2**	
Тема 3.1. Будущее информационной безопасности	**Содержание учебного материала**	***2***	ОК 01, ОК 02, ОК 04, ОК 09
	1. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.	2	
	В том числе практических и лабораторных занятий		
	Самостоятельная работа обучающегося завершение и оформление отчетов по лабораторным и практическим работам	**1**	
	Итоговое занятие	***2***	
	Экзамен	***6***	
Всего:		**72**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Описание материально-технической базы, необходимой для осуществления образовательного процесса

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащённость специальных помещений и помещений для самостоятельной работы
1	Учебная аудитория для проведения занятий всех видов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: 414056, Астраханская область, городской округ город Астрахань, г. Астрахань, ул. Татищева, строение 18а/1, 55,2 кв.м., 1 этаж, помещение № 12	1. Автоматизированные рабочие места на 14 обучающихся 2. Автоматизированное рабочее место преподавателя 3. 14 комплектов компьютерных комплектующих для произведения сборки, разборки и сервисного обслуживания ПК и оргтехники 4. Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения 5. Стационарный мультимедийный комплект (проектор, экран) 6. Доска учебная 7. Комплект учебной мебели на 25 обучающихся 8. Учебные наглядные пособия 9. Программное обеспечение общего и профессионального назначения. 10. Доступ к информационно-телекоммуникационной сети «Интернет»
2	Помещение для самостоятельной и воспитательной работы: 414056, Астраханская область, городской округ город Астрахань, г. Астрахань, ул. Татищева, строение 18а/1, 221,1 кв.м., 2 этаж, помещение № 7	1. Комплект учебной мебели на 50 чел. 2. Комплект учебно-наглядных пособий 3. Компьютеры - 8 шт. 4. Стационарный мультимедийный комплект (проектор, экран) 5. Доступ к информационно-телекоммуникационной сети «Интернет»

3.2. Рекомендуемая литература

а) основная учебная литература:

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

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

3. 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

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

б) дополнительная учебная литература:

1. Кудинов, Ю. И. Практикум по основам современной информатики: учебное пособие для спо / Ю. И. Кудинов, Ф. Ф. Пащенко, А. Ю. Келина. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 352 с. — ISBN 978-5-8114-8252-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/173799

2. Бильфельд, Н. В. Методы MS EXCEL для решения инженерных задач : учебное пособие для спо / Н. В. Бильфельд, М. Н. Фелькер. — 2-е, стер. — Санкт-Петербург : Лань, 2021. — 164 с. — ISBN 978-5-8114-7573-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162380

в) перечень учебно-методического обеспечения:

г) интернет-ресурсы:

1. Информационная система «Единое окно доступа к образовательным ресурсам». [Электронный ресурс]. Режим доступа: http://window.edu.ru/

д) электронно-библиотечные системы:

1. Электронно-библиотечная система «IPRbooks» (http://www.iprbookshop.ru)
2. Образовательно-издательский центр «Академия» (https://academia-library.ru)

3.3. Особенности организации обучения для инвалидов и лиц с ограниченными возможностями здоровья

Для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья на основания письменного заявления учебная дисциплина « Основы информационной безопасности» реализуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья (далее – индивидуальных особенностей).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения	***Критерии оценки***	***Методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины:		
- 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	- 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	- оценка качества знаний при выполнении практических работ; - анализ деятельности обучающихся в процессе выполнения аудиторных и внеаудиторных заданий; - экспертная оценка по результатам наблюдения за деятельностью студента в процессе освоения учебной дисциплины

работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с 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	выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные средства и устройства информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в профессиональной деятельности в том числе с 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	

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;	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	

- 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 безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.	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; 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;	
Перечень умений, осваиваемых в рамках дисциплины:		
распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; - определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; - оценивать практическую значимость результатов поиска; - оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное	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;	- оценка качества знаний при выполнении практических работ; - анализ деятельности обучающихся в процессе выполнения аудиторных и внеаудиторных заданий; - экспертная оценка по результатам наблюдения за деятельностью студента в процессе освоения учебной дисциплины

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.	