

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Соловьев Андрей Александрович
Должность: ректор ФГБОУ ВО Вавиловский университет
Дата подписания: 29.10.2026 07:34:24
Уникальный программный ключ:
528682d78e671e566ab07f01fe1ba2172f755a12

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Саратовский государственный университет генетики,
биотехнологии и инженерии имени Н.И. Вавилова»
Пугачевский филиал



Утверждаю

Директор Пугачёвского филиала

/Семенова О.Н./

«25» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина	ОП.06 Основы информационной безопасности
Специальность	09.02.12 Техническая эксплуатация и сопровождение информационных систем
Квалификация выпускника	специалист по технической эксплуатации и сопровождению информационных систем
Нормативный срок обучения	2 года 10 месяцев на базе основного общего образования
Форма обучения	Очная

Программа учебной дисциплины ОП.06 Основы информационной безопасности разработана на основе:

- федерального государственного образовательного стандарта среднего профессионального образования 09.02.12 Техническая эксплуатация и сопровождение информационных систем;
- примерной рабочей программы общепрофессиональной дисциплины «ОП.06 Основы информационной безопасности»;
- учебного плана по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем;
- рабочей программы воспитания по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем

Организация-разработчик: Пугачёвский гидромелиоративный техникум имени В. И. Чапаева – филиал ФГБОУ ВО «Саратовский государственный университет генетики, биотехнологии и инженерии имени Н.И. Вавилова»

Разработчик: Илюшенко М.Ю. преподаватель высшей квалификационной категории

Рассмотрено на заседании цикловой комиссии агротехнических дисциплин
Протокол № 7 от «24» февраля 2026 г.

Председатель цикловой комиссии  /Балабекова А. И./

Рекомендовано методическим Советом филиала к использованию в учебном процессе
Протокол № 4 от «25» февраля 2026 г.

Председатель методического совета  /Семенова О. Н./

Рассмотрено и одобрено на педагогическом совете филиала
Протокол № 4 от «25» февраля 2026 г.

Председатель педагогического совета  /Семенова О. Н./

СОДЕРЖАНИЕ	стр.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ	9
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ	12
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ	14

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ 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 (п. 4.3 ПОП).

В результате освоения дисциплины обучающийся должен¹:

Код ОК, ПК	Уметь	Знать	Владеть навыками
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;	– 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;	-
	– составлять план действия; определять необходимые ресурсы;	– 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	
	– владеть актуальными методами работы в профессиональной и смежных сферах	-	-
	– реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	-	-
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	– лексический минимум,	-

	профессиональные темы	относящийся к описанию предметов, средств и процессов профессиональной деятельности	
ПК 1.7	<ul style="list-style-type: none"> – идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС 	<ul style="list-style-type: none"> – основы ИБ организации – модель угроз информационной безопасности ИС организации заказчика – процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика – основы администрирования СУБД – основы системного администрирования – Коммуникационное оборудование – сетевые протоколы – Основы современных операционных систем – устройство и функционирование современных ИС – основы архитектуры мультиарендного программного обеспечения 	<ul style="list-style-type: none"> – распознавание инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – передача информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – информирование заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – временное блокирование доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС

ПК 2.5	<ul style="list-style-type: none"> – идентифицировать инциденты ИБ при работе с БД – осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации) – управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ – устанавливать и сопровождать антивирусное ПО 	<ul style="list-style-type: none"> – понятие и классификация инцидентов ИБ – типичные угрозы ИБ при работе с БД – процедуры и регламенты передачи информации об инцидентах в службу ИБ организации – средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры) – основы работы со средствами антивирусной защиты – основы ИБ – основы деловой этики – правила деловой переписки 	<ul style="list-style-type: none"> – распознавание инцидентов ИБ при работе с БД – формирование перечня инцидентов ИБ – передача информации об инцидентах в службу ИБ организации – временное блокирование доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости) – поддержание баз антивирусных программ в актуальном состоянии
--------	--	---	---

1.3. Количество часов, отводимое на освоение программы учебной дисциплины

Объем образовательной нагрузки обучающегося 76 часов,
в том числе: аудиторных часов: 44 часа:
в форме практической подготовки 20 часов;

2. СТРУКТУРА И СОДЕРЖАНИЕ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	<i>Объем в часах</i>
Объем образовательной программы дисциплины	76
в т.ч.	
Основное содержание	76
в т. ч.:	
теоретическое обучение	44
практические занятия	20
Промежуточная аттестация (экзамен)	12

2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем часов	Формируемые компетенции
Раздел 1. Теоретические основы информационной безопасности		14	
Тема 1.1. Введение в информационную безопасность	Содержание: Основные понятия и определения (ИБ, защита информации, угроза, уязвимость, риск). История и развитие ИБ. Место ИБ в профессиональной деятельности. Категории информации (конфиденциальная, персональные данные, коммерческая тайна).	4	ОК 01, ОК 02
Тема 1.2. Угрозы информационной безопасности	Содержание: Классификация угроз (внутренние, внешние, случайные, умышленные). Источники угроз. Модель угроз ИС организации заказчика. Основные виды атак (DDoS, MITM, фишинг, социальная инженерия).	4	ОК 01, ОК 02, ПК 1.7
	Практические занятия: Анализ модели угроз для типовой информационной системы. Классификация угроз по категориям.	2	ОК 01, ОК 02
Тема 1.3. Нормативно-правовое регулирование в области ИБ	Содержание: Законодательство РФ (152-ФЗ «О персональных данных», 149-ФЗ «Об информации»). Стандарты ISO 27001, GDPR. Политика информационной безопасности организации.	4	ОК 01, ОК 09
Раздел 2. Технические и программные средства защиты информации		20	
Тема 2.1. Криптографические методы защиты	Содержание: Основы криптографии: симметричные и асимметричные алгоритмы. Хеширование и цифровая подпись. Применение криптографии в приложениях. Стеганография.	4	ОК 02, ПК 1.7

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем часов	Формируемые компетенции
	Практические занятия: Работа с симметричными и асимметричными алгоритмами. Хеширование и создание цифровой подписи сообщения. Шифрование данных с помощью openssl.	4	ОК 02, ПК 1.7
Тема 2.2. Защита сетевой инфраструктуры	Содержание: Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.). Использование VPN и межсетевых экранов (firewall). Протоколы SSL/TLS, SSH, Kerberos.	4	ОК 02, ПК 1.7
	Практические занятия: Организация защиты от атак. Настройка VPN и межсетевого экрана. Настройка SSH-ключей и безопасного подключения.	4	ОК 02, ПК 1.7
Тема 2.3. Безопасность приложений и баз данных	Содержание: Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей. Защита баз данных от внешних угроз.	4	ОК 02, ПК 1.7, ПК 2.5
Раздел 3. Организация защиты информации на предприятии		18	
Тема 3.1. Управление доступом и аутентификация	Содержание: Методы аутентификации и авторизации (пароли, сертификаты, биометрия). Многофакторная аутентификация (MFA). Управление правами доступа пользователей.	4	ОК 01, ОК 02, ПК 2.5
	Практические занятия: Настройка многофакторной аутентификации. Разграничение прав доступа к базе данных.	2	ОК 02, ПК 2.5
Тема 3.2. Защита данных и резервное копирование	Содержание: Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным. Принципы безопасности хранения данных.	4	ОК 02, ПК 2.5

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем часов	Формируемые компетенции
	Практические занятия: Выполнение резервного копирования и восстановления данных. Настройка шифрования данных. Управление доступом к данным.	4	ОК 02, ПК 2.5
Тема 3.3. Безопасность облачных технологий	Содержание: Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасность. Разделение ответственности в облаке.	4	ОК 02
Раздел 4. Инциденты информационной безопасности и реагирование на них		12	
Тема 4.1. Обнаружение и классификация инцидентов ИБ	Содержание: Понятие и классификация инцидентов ИБ. Типичные угрозы при работе с БД. Процедуры и регламенты передачи информации об инцидентах в службу ИБ организации.	4	ОК 02, ПК 1.7, ПК 2.5
	Практические занятия: Идентификация инцидентов ИБ при работе с ИС. Формирование перечня инцидентов. Передача информации об инцидентах в службу ИБ.	4	ОК 02, ПК 1.7, ПК 2.5
Тема 4.2. Реагирование на инциденты и цифровая криминалистика	Содержание: Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика (форензика). Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT.	2	ОК 02, ПК 1.7
Тема 4.3. Социальная инженерия и человеческий фактор	Содержание: Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности. Разработка политики информационной безопасности.	2	ОК 01, ОК 09
Промежуточная аттестация: Экзамен		12	

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем часов	Формируемые компетенции
ВСЕГО:		76	

3. Условия реализации программы учебной дисциплины

3.1 Для реализации программы дисциплины предусмотрены следующие специальные помещения:

Рабочее место преподавателя, рабочие места обучающихся, доска магнитно-маркерная 100*180, системный блок BigTech 5NG Core i5 12400F, H610, 16Gb, 500Gb, RTX 3050 8Gb, 500W – 11 шт., монитор Xiaomi A27i27/FHD/IPS/100Hz/250cd/

HDMI/DP(ELA5345EU) – 11 шт., проектор Acer X1228H, черный (mr.jthcd.001), 111" Экран для проектора Cactus WallExpert CS-PSWE-200*200-WT

Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду университета, выходом в информационно-коммуникационную сеть «Интернет», обеспечены контентной фильтрацией, специализированным программным обеспечением.

Лицензионное программное обеспечение:

1) «P7-Офис». Договор № ЦЗ-1К-033 от 21.12.2022 г. с ООО «Солярис Технолоджис», г. Саратов (с 01.01.2023, бессрочно).

2) Kaspersky Endpoint Security (антивирусное программное обеспечение). Договор № 6-441025/КСП-170 от 22.12.2025 г. с ООО «Солярис Технолоджис», г. Саратов (01.01.2026 - 31.12.2026).

3. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организацией выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные 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>

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>

3.2.2. Дополнительная литература:

Печатные издания

1. Михеева Е.В. Информационные технологии в профессиональной деятельности. – М.: «Академия», 2014. Гриф ФИРО.

2. Цветкова М.С. Хлобыстова И.Ю. Информатика. – 6-е изд., стер. – М. Издательский центр «Академия», 2020.

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>

Интернет - ресурсы:

1. **Stepik. Курсы по архитектуре ЭВМ и операционным системам**

<https://stepik.org/search?query=операционные%20системы>

2. **Operating Systems: Three Easy Pieces (русская версия):**

<https://pages.cs.wisc.edu/~remzi/OSTEP/>

3. **OpenEdu. Курсы по архитектуре компьютеров и системному программированию:**

<https://openedu.ru/>

4. OpenEdu (Открытое образование). Национальная платформа онлайн-курсов российских вузов. Содержит курсы по информатике, тестированию, алгоритмам и интерфейсам ИС. <https://openedu.ru/>

3.2.3. Информационные технологии, используемые при осуществлении образовательного процесса:

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине:

- персональные компьютеры, посредством которых осуществляется доступ к информационным ресурсам и оформляются результаты самостоятельной работы;
- проекторы и экраны для демонстрации слайдов мультимедийных лекций;
- активное использование средств коммуникаций (электронная почта, тематические сообщества в социальных сетях и т.п.).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения общеобразовательной дисциплины раскрываются через дисциплинарные результаты, направленные на формирование общих и профессиональных компетенций по разделам и темам содержания учебного материала

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 поиска информации, современные средства и устройства	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;	Экспертное наблюдение выполнения практических работ и видов работ по практике Устный опрос Диагностика (тестирование, контрольные работы) Промежуточная аттестация: экзамен

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

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

<p>алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети;</p> <p>- основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</p> <p>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;</p>	<p>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;</p> <p>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;</p> <p>Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</p> <p>Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части;</p> <p>Умеет определять этапы решения задачи;</p>	
--	--	--

<ul style="list-style-type: none"> - 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 	<p>Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;</p> <p>Составляет план действия;</p> <p>Может определять необходимые ресурсы;</p> <p>Владеет актуальными методами работы в профессиональной и смежных сферах;</p> <p>Может реализовывать составленный план;</p> <p>Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника);</p> <p>Умеет определять задачи для поиска информации;</p> <p>Умеет определять необходимые источники информации;</p> <p>Планирует процесс поиска;</p> <p>Умеет структурировать получаемую информацию;</p> <p>Может выделить наиболее значимое в перечне информации;</p> <p>Умеет оценивать практическую значимость результатов поиска;</p> <p>Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач;</p> <p>Может использовать современное программное обеспечение;</p> <p>Может использовать</p>	
--	--	--

<p>цифровые средства для решения профессиональных задач;</p> <ul style="list-style-type: none"> - 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. 	<p>различные цифровые средства для решения профессиональных задач;</p> <p>Понимает тексты на базовые профессиональные темы;</p> <p>Умеет шифровать данные и обеспечивать их конфиденциальность;</p> <p>Умеет анализировать требования безопасности информационных систем;</p> <p>Может разрабатывать и реализовывать меры безопасности;</p> <p>Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.</p>	
---	---	--