

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Соловьев Дмитрий Александрович

Должность: ректор ФГБОУ ВО Вавиловский университет

Дата подписания: 19.10.2026 09:37:28

Уникальный программный ключ:

528682d78e671e566ab07f8b4b2173f735a12

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

Краснокутский зооветеринарный техникум – филиал

**Федерального государственного бюджетного образовательного учреждения высшего
образования «Саратовский государственный университет генетики, биотехнологии и
инженерии имени Н.И. Вавилова»**

УТВЕРЖДАЮ

Директор Краснокутского филиала

/Ткачева Г.М./

«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
Срок получения СПО	2 года 10 месяцев на базе основного общего образования
Форма обучения	Очная

г. Красный Кут -2026

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

- федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, утвержденного Приказом Министерства просвещения Российской Федерации от 10 марта 2025 года № 184.

- примерной рабочей программы учебной дисциплины «Основы информационной безопасности» по технологическому профилю;

- 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: Краснокутский зооветеринарный техникум - филиал федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный университет генетики, биотехнологии и инженерии имени Н.И. Вавилова».

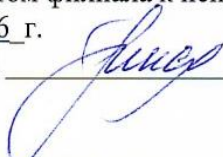
Разработчик: Пичайкина Т.В., преподаватель.

Рассмотрена на заседании цикловой комиссии экономических и технологических дисциплин,

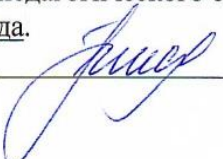
протокол № 7 от «18» февраля 2026 года.

Председатель цикловой комиссии  / Рыжкова В.П./

Рекомендовано методическим Советом филиала к использованию в учебном процессе, протокол № 4 от «20» февраля 2026 г.

Председатель методического совета  / Ткачева Г.М./

Рассмотрено и одобрено на заседании педагогического совета техникума, протокол № 5 от «25» февраля 2026 года.

Председатель педагогического совета  / Ткачева Г.М./

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ.....	10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	12

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.06 Основы информационной безопасности»

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 в соответствии с ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

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	Владеть навыками
ОК.01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	-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 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	-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 Пользоваться профессиональной документацией на государственном и иностранном языках	-понимать тексты на базовые профессиональные темы	-лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.7 Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем	-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	-основы ИБ организации -модель угроз информационной безопасности ИС -процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика -основы администрирования СУБД -основы системного администрирования коммуникационное оборудование -сетевые протоколы	-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

	процессов создания (модификации) и сопровождения ИС -настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	-основы современных операционных систем -устройство и функционирование современных ИС -основы архитектуры мультиарендного программного обеспечения	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 Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных	-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	-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	-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

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	46
<i>в том числе:</i>	
теоретическое обучение	22
практические занятия	24
Самостоятельная работа	-
Промежуточная аттестация в форме дифференцированного зачета	
Всего	46

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятий	Объем, акад. ч. / в том числе в форме практической подготовки, акад. ч	Осваиваемые элементы ОК и ПК
Тема 1. Введение в информационную безопасность	Содержание	2	ОК 01 ОК 02 ОК09
	1.Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2	
Тема 2. Управление безопасностью информации	Содержание	2	ОК 01 ОК 02 ОК09 ПК 1.7
	2.Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
Тема 3. Криптография	Содержание	6	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	3.Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических и лабораторных занятий	4	
	1. Работа с симметричными и асимметричными алгоритмами.	2	
	2.Хэширование и создание цифровой подписи сообщения.	2	
Тема 4. Защита сетевой инфраструктуры	Содержание	6	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	4.Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	
	В том числе практических и лабораторных занятий		
	3. Организация защиты от атак	2	
	4. Организация работы VPN и межсетевого экрана	2	
Тема 5. Безопасность приложений	Содержание	4	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	5.Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе практических и лабораторных занятий		

	5. Тестирование на проникновение и анализ уязвимостей.	2	
Тема 6. Защита данных	Содержание	8	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	6.Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	
	В том числе практических и лабораторных занятий	6	
	6. Выполнение резервного копирования	2	
	7. Выполнение восстановления данных	2	
	8. Управление доступом к данным	2	
Тема 7. Безопасность облачных технологий	Содержание	6	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	7.Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2	
	В том числе практических и лабораторных занятий	4	
	9. Изучение модели облачных услуг и их безопасности	2	
	10.Работа с различными моделями облачных услуг	2	
Тема 8. Инциденты безопасности	Содержание	6	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	8.Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента.	2	
	9.Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	
	В том числе практических и лабораторных занятий	2	
	11. Работа с инцидентами.	2	
Тема 9. Социальная инженерия и человеческий фактор	Содержание	4	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	10.Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	
	В том числе практических и лабораторных занятий	2	
	12. Разработка политики информационной безопасности	2	
Тема 10. Будущее информационной безопасности	Содержание	2	ОК 01 ОК 02 ОК09 ПК 1.7 ПК 2.5
	11.Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2	
Промежуточная аттестация в форме дифференцированного зачета			
Всего		46	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Учебная аудитория для проведения учебных занятий – кабинет «Информатика» №22, оснащенная оборудованием и техническими средствами обучения по специальности 09.02.07 «Информационные системы и программирование».

Рабочее место преподавателя, рабочие места обучающихся, доска меловая, компьютеры в комплекте с лицензионным программным обеспечением (монитор XiaomiA27i 27/FHD/IPS/100Hz/250cd/HDMI/DP (ELA5345EU), системный блок BigNech 5 NGCorei5 12400F) -13 шт., проектор BenQProjectorMP622C, экран переносной APOLLOScreenMedia. Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду университета, выходом в информационно-коммуникационную сеть «Интернет», обеспечены контентной фильтрацией, специализированным программным обеспечением.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

3.2.1. Основная 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>

3.2.2. Дополнительные источники

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва: ИНФРА-М, 2026. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-16-021164-0. - Текст: электронный. - URL: <https://znanium.ru/catalog/product/2207574>

3.2.3. Нормативные правовые акты и государственные стандарты

1. Федеральный закон № 152-ФЗ от 27 июля 2006 г. «О персональных данных»
2. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации»

3. Постановление Правительства РФ № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»

4. Приказ ФСБ России № 378 от 10 июля 2014 г. «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»

5. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

6. Национальный стандарт Российской Федерации ГОСТ Р 53114- 2008 «Информационная безопасность сетей связи общего пользования. Общие положения»

7. Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовая. Платежные приложения. Требования по защите конфиденциальной информации держателей платежных карт»

8. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»

9. Стандарты серии ISO/IEC 27000 («Система менеджмента информационной безопасности»).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости компетенций	Методы оценки
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	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 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	Подготовка, выступление с докладом, сообщением, презентацией Наблюдение за выполнением практического задания (деятельностью студента) Защита отчетов по практическим и лабораторным работам Дифференцированный зачет

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,	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	
---	--	--

таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. 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.	и НІРАА; 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; 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; 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.	
--	--	--