МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ
«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ РАДИОЭЛЕКТРОНИКИ, ИНФОРМАЦИОННЫХ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»
(ГБПОУ РО «РКРИПТ»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность:
09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Квалификация выпускника:
ПРОГРАММИСТ

Форма обучения: очная

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 21691819b3fb1e1c5127004fe138badf
Владелец: Лепёшкин Дмитрий Владимирович
Действителен: с 05.02.2026 г. по 01.05.2027 г.

Ростов-на-Дону
2026

СОГЛАСОВАНО
И.о. заместителя директора
по учебно-методической работе
_____ М.В. Шевченко
«__» апреля 2026 г.

УТВЕРЖДАЮ
Директор колледжа
_____ Д.В. Лепёшкин
«__» апреля 2026 г.

РАССМОТРЕНО
Цикловой комиссией программирования компьютерных систем
Протокол № 8 от «20» марта 2026 г.
Председатель ЦК А.Е. Нецветаева

Рабочая программа дисциплины ОП.05 Основы информационной безопасности разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Минпросвещения России от 24.02.2025 №138 (зарегистрировано в Минюсте России 31.03.2025 №81696); с учетом примерной образовательной программы подготовки специалистов среднего звена по специальности и профессиональным стандартом 06.001 Программист.

Разработчик(и):
Махно Л.В., преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ»

Рецензенты:
Галкина Н.Г., преподаватель высшей квалификационной категории ГБПОУ РО «РКРИПТ»
Медяников А.А., генеральный директор ООО «Инкост»

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины ОП.05 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 ОП.05 Основы информационной безопасности включена в обязательную часть общепрофессионального цикла образовательной программы.

1.2. Планируемые результаты освоения дисциплины

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

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	**Уметь**	**Знать**	**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; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-

ОК.02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	-
ОК.09	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.1	-	принципы безопасности хранения данных	-
ПК 1.4	-	методы защиты баз данных от внешних угроз	-
ПК 1.5	шифровать данные и обеспечивать их конфиденциальность	принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. методы аутентификации и авторизации пользователей, включая использование	-

		паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	
ПК 3.1	-	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности	-
		современный отечественный и зарубежный опыт в профессиональной деятельности	-
ПК 3.2	-	принципы и методы обеспечения безопасности информационных систем	-
ПК 3.3	анализ требований безопасности информационных систем	принципов безопасности информационных систем современных методов и технологий в области безопасности информационных систем законодательных и нормативных актов в области безопасности информационных систем	применение современных методов и технологий в области безопасности информационных систем
ПК 3.5	-	источники угроз информационной безопасности и меры по их предотвращению	-
ПК 3.7	разрабатывать и реализовывать меры безопасности реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	основные угрозы безопасности мобильных приложений принципы криптографии и шифрования данных. стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA основные принципы безопасности информации и методов ее защиты. стандартные криптографические	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 несанкционированного доступа.

		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	обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS соблюдение законодательства и регуляций в области защиты данных

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки
Учебные занятия	62	38
Самостоятельная работа	-	-
Промежуточная аттестация в форме дифференцированного зачета	2	2
Всего	**64**	**40**

2.2. Содержание дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч.	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности		**64**	
Тема 1.1. Введение в информационную безопасность	**Содержание**	**2**	ОК.01 ОК.02 ОК.09 ПК 1.1 ПК 3.2
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности.	2	
Тема 1.2. Управление безопасностью информации	**Содержание**	**6**	ОК.01 ОК.02 ОК.09 ПК 3.1
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
	В том числе практических и лабораторных занятий	**4**	
	1. Изучение правовых документов государственной политики в сфере информационной безопасности.	4/4	
Тема 1.3. Криптография	**Содержание**	**6**	ОК.01 ОК.02 ОК.09 ПК 1.5 ПК 3.7
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических и лабораторных занятий	**4**	
	2. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	4/4	
Тема 1.4. Защита сетевой инфраструктуры	**Содержание**	**12**	ОК.01 ОК.02 ОК.09 ПК 3.5 ПК 3.7
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов. Угрозы при работе в беспроводных сетях. Стандарты из семейства 802.11x. Управление подключениями в точке беспроводного доступа	2	
	В том числе практических и лабораторных занятий	**10**	
	3. Организация защиты от атак.	4/4	
	4. Организация работы VPN и межсетевого экрана.	4/4	
	5. Настройка защищенного беспроводного соединения.	2/2	
	Содержание	**8**	

Тема 1.5. Безопасность приложений	Методы классификации компьютерных вирусов. Анализ программной структуры компьютерных вирусов. Основные методы защиты информации от компьютерных вирусов. Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	ОК.01 ОК.02 ОК.09 ПК 1.1 ПК 1.4
	В том числе практических и лабораторных занятий	**6**	
	6. Тестирование на проникновение и анализ уязвимостей.	2/2	
	7. Установка и изучение возможностей антивирусных программ	4	
Тема 1.6. Защита данных	**Содержание**	**8**	ОК.01 ОК.02 ОК.09 ПК 1.4 ПК 3.2
	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**	
	8. Выполнение резервного копирования и восстановления данных. Управление доступом к данным	4/4	
	9. Настройка параметров безопасности. Установка параметров шифрования	2/2	
Тема 1.7. Безопасность облачных технологий	**Содержание**	**6**	ОК.01 ОК.02 ОК.09 ПК 1.4 ПК 3.7
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2	
	В том числе практических и лабораторных занятий	**4**	
	10. Изучение модели облачных услуг и их безопасности	4/4	
Тема 1.8. Инциденты безопасности	**Содержание**	**6**	ОК.01 ОК.02 ОК.09 ПК 3.5 ПК 3.7
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	
	В том числе практических и лабораторных занятий	**4**	
	11. Работа с инцидентами.	4/4	
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание**	**6**	ОК.01 ОК.02 ОК.09 ПК 3.2 ПК 3.3
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	
	В том числе практических и лабораторных занятий	**4**	
	12. Разработка политики информационной безопасности	4/4	
Тема 1.10. Будущее информационной безопасности	**Содержание**	**2**	ОК.01 ОК.02 ОК.09 ПК 3.2 ПК 3.3
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2	

Дифференцированный зачет	**2/2**	ОК.01, ОК.02, ОК.09 ПК 1.1, ПК 1.4 ПК 1.5, ПК 3.1 ПК 3.2, ПК 3.3 ПК 3.5, ПК 3.7
Всего	**64**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная:

Посадочные места по количеству обучающихся (столы, стулья).

Рабочее место преподавателя.

Шкаф для хранения учебной и методической литературы.

Доска маркерная.

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.

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.

Программное обеспечение (MS Windows 10; MS Office 2016; Adobe Reader; PgAdmin 4; Open Server; VS Code, Visual Studio Community, Oracle Virtual Box, 1C Enterprise 8.3)

Мультимедийное оборудование (персональный компьютер преподавателя, коммутатор).

Методические материалы, плакаты и информационные стенды.

Библиотека, читальный зал с выходом в Интернет.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Мельников, В. П. Информационная безопасность.: учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва: КноРус, 2025. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.04.2026). — Текст : электронный.

2. Бабаш, А. В. Информационная безопасность. Лабораторный практикум + еПриложение : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2025. — 131 с. — ISBN 978-5-406-14215-8. — URL: https://book.ru/book/956850 (дата обращения: 08.04.2026). — Текст: электронный.

3. Медведев, В. А. Информационная безопасность. Введение в специальность + еПриложение:Тесты: учебник / В. А. Медведев. — Москва: КноРус, 2024. — 143 с. — ISBN

978-5-406-12625-7. — URL: https://book.ru/book/951878 (дата обращения: 08.04.2026). — Текст: электронный.

4. Пестунова, Т. М. Информационная безопасность и защита информации: краткое введение и практикум : учебное пособие / Т. М. Пестунова, А. А. Перов. — Москва: Русайнс, 2025. — 132 с. — ISBN 978-5-466-10397-7. — URL: https://book.ru/book/960807 (дата обращения: 08.04.2026). — Текст: электронный.

3.2.2. Дополнительные источники

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)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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;	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;	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

- 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;	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;	

- 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	Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области	

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;	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;	

- понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. ***Умеет:*** -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно	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);	

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	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.	двухфакторную аутентификацию.	