Автономная некоммерческая организация профессионального образования
«Международный техникум экономики, права
и информационных технологий»

УТВЕРЖДАЮ
Директор АНОПО «МТЭПИТ»

_____ /В.П. Анисимов/
«06» 04 2026 г.

РАБОЧАЯ ПРОГРАММА ОБЩЕПРОФЕССИОНАЛЬНОЙ ДИСЦИПЛИНЫ ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОП. Общепрофессиональные дисциплины
П. Профессиональный цикл

по специальности
09.02.12 Техническая эксплуатация и сопровождение информационных систем

Форма обучения: очная, заочная

Воронеж
2026 г.

РАССМОТРЕНО И ОДОБРЕНО ПЦК ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

Протокол № 12 от «06» 04 2026 г.

Председатель ПЦК  Шелудякова Т.В.

подпись инициалы и фамилия

Начальник УМО  Прокофьева Н.А.

подпись инициалы и фамилия

Разработчики:

Матыцина И.А., к.т.н., доцент преподаватель

Ф.И.О., ученая степень, звание, должность

Эксперты:

преподаватель

Ф.И.О., ученая степень, звание, должность

преподаватель

Ф.И.О., ученая степень, звание, должность

Рабочая программа учебной дисциплины ОП.06. Основы информационной безопасности разработана с учетом методических рекомендаций по разработке рабочих программ дисциплин циклов ОГСЭ.00, ЕН.00, П.00 программы подготовки специалистов среднего звена на основе Приказа Минпросвещения России от 10.03.2025 № 184 "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем" (Зарегистрировано в Минюсте России 14.04.2025 № 81849).

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ..... ERROR! BOOKMARK NOT DEFINED.

1.1. Цель и место дисциплины в структуре образовательной программы **Error! Bookmark not defined.**

1.2. Планируемые результаты освоения дисциплины ..... **Error! Bookmark not defined.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ ERROR! BOOKMARK NOT DEFINED.

2.1. Трудоемкость освоения дисциплины ..... **Error! Bookmark not defined.**

2.2. Примерное содержание дисциплины ..... **Error! Bookmark not defined.**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ..... ERROR! BOOKMARK NOT DEFINED.

3.1. Материально-техническое обеспечение ..... **Error! Bookmark not defined.**

3.2. Учебно-методическое обеспечение ..... **Error! Bookmark not defined.**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ..... ERROR! BOOKMARK NOT DEFINED.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ОБЩЕПРОФЕССИОНАЛЬНОЙ ДИСЦИПЛИНЫ ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины ОП.06 Основы информационной безопасности: формирование представлений об устройстве компьютера; изучить конструкции и функции различных элементов компьютеров, предназначенных для хранения и обработки информации, рассмотреть компоненты компьютера, которые получают информацию от внешних источников и отсылают результаты вычислений внешним приемникам данных.

Дисциплина ОП.06 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;	– 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	– алгоритмы выполнения работ в профессиональной и	-

	ресурсы;	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	– 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.	-

	обеспечение; использовать различные цифровые средства для решения профессиональных задач		
ОК. 09	– понимать тексты на базовые профессиональные темы	– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.7	– 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	– 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	– 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	– 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

1.3. Количество часов на освоение программы учебной дисциплины ОП.06 Основы информационной безопасности:

Очная форма обучения:

максимальная учебная нагрузка 36 часов, в том числе:
- обязательная аудиторная учебная нагрузка 36 часов.

Заочная форма обучения:

максимальная учебная нагрузка 36 часов, в том числе:
- обязательная аудиторная учебная нагрузка 10 часов;
- самостоятельная работа 26 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ОБЩЕПРОФЕССИОНАЛЬНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы очной формы обучения

Вид учебной работы по очной форме обучения	*Объем часов*
Максимальная учебная нагрузка (всего)	*36*
Обязательная аудиторная учебная нагрузка (всего)	*36*
в том числе:	
3 семестр	
из них:	
лекции	*26*
лабораторные занятия	*10*
Промежуточная аттестация	*Дифференцированный зачет*

Объем учебной дисциплины и виды учебной работы заочной формы обучения

Вид учебной работы по очной форме обучения	*Объем часов*
Максимальная учебная нагрузка (всего)	*36*
Обязательная аудиторная учебная нагрузка (всего)	*10*
Самостоятельная работа	*26*
в том числе:	
3 семестр	
из них:	
лекции	*6*
лабораторные занятия	*4*
Промежуточная аттестация	*Домашняя к/р Дифференцированный зачет*

2.2. Тематический план и содержание учебной дисциплины ОП.06. Основы информационной безопасности

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий	Объем часов			Формируемые компетенции
		ОФО	ЗФО		
		Ауд. зан.	Ауд. зан.	Сам. раб.	
		36	**10**	**26**	
	3 СЕМЕСТР (очная форма обучения) 4 СЕМЕСТР (заочная форма обучения)				
Тема 1. Введение в информационную безопасность	**Содержание**				
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	4	1		ОК 01 ОК 09 ПК 1.7 ПК 2.5
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 2. Управление безопасностью информации	**Содержание**				
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	4	1		
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 3. Криптография	**Содержание**				
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	4	1		
	В том числе практических и лабораторных занятий				
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2			
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 4. Защита сетевой инфраструктуры	**Содержание**				
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2			
	В том числе практических и лабораторных занятий				

	Организация защиты от атак	1			
	Организация работы VPN и межсетевого экрана				
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 5. Безопасность приложений	**Содержание**				
	Уязвимости веб-приложений (OWASP TopTen). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	1		
	В том числе практических и лабораторных занятий				
	Тестирование на проникновение и анализ уязвимостей.	1			
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 6. Защита данных	**Содержание**				
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	1		
	В том числе практических и лабораторных занятий				
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	1	1		
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 7. Безопасность облачных технологий	**Содержание**				
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2			
	В том числе практических и лабораторных занятий				
	Изучение модели облачных услуг и их безопасности	1	1		
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 8. Инциденты безопасности	**Содержание**				
	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				
	Работа с инцидентами.	1	1		

	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			2	
Тема 9. Социальная инженерия и человеческий фактор	**Содержание**				
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	1		
	В том числе практических и лабораторных занятий				
	Разработка политики информационной безопасности	1	1		
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			4	
Тема 10. Будущее информационной безопасности	**Содержание**				
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2			
	В том числе самостоятельная работа обучающихся *Необходимость и тематика определяются образовательной организацией*			4	
Промежуточная аттестация: дифференцированный зачет(очная форма обучения); домашняя к/р и дифференцированный зачет (заочная форма обучения)					
Всего:		**36**	**10**	**26**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 **Требования к минимальному материально-техническому обеспечению**

Реализация программы учебной дисциплины требует наличия учебной лаборатории архитектуры персонального компьютера и периферийных устройств.

Оборудование учебного кабинета:

- посадочные места по количеству студентов;
- рабочее место преподавателя;

Технические средства обучения:

- компьютер;
- проектор и экран;
- операционная система Windows 2003/XP;
- системы распознавания информации;
- текстовый процессор Microsoft Word;
- табличный процессор Microsoft Excel;
- программа подготовки презентаций Microsoft Power Point;
- модем, выход в INTERNET

Наглядные пособия:

- комплект учебно-наглядных пособий по дисциплине Основы информационной безопасности;
- образцы выполнения практических и контрольных заданий;
- материалы для лабораторных, практических работ;

Обучающие средства:

- инструкции для практических работ;
- инструкции для лабораторных работ;
- методический материал для уроков;
- методические материалы для выполнения расчётно-графических работ;
- методические материалы для самостоятельной внеаудиторной работы студентов.

Контрольные материалы:

- тесты по темам;
- контрольные задания;
- пакет контрольных вопросов для дифференцированного зачета.

3.2. Информационное обеспечение обучения:

Основная литература

1. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2026. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510
2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082

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
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

Интернет-ресурсы:

1. Anti-Malware.ru. Категории средств защиты информации, аналитика рынка кибербезопасности [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/
2. Cyber Security Base. Бесплатный онлайн-курс [Электронный ресурс]. – Режим доступа: https://cybersecuritybase.mooc.fi/
3. Open Security Training — Into to Security Coding. Безопасное программирование и оценка уязвимостей [Электронный ресурс]. – Режим доступа: https://training.opensecurity.com/

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, проектов, исследований.

Результаты обучения	Показатели освоенности компетенций	Методы оценки
Знает: - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; -основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и	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	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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;	использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности;	

- 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 OpenIDConnect; - 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	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 OpenIDConnect; 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;	

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. ***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	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	

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	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;	

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, сессионныетокены и двухфакторную аутентификацию.	Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионныетокены и двухфакторную аутентификацию.	