

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Узунова Г.П.  
Должность: Директор  
Дата подписания: 22.06.2026 11:40:37  
Уникальный программный ключ:  
0dd9ff38cdb9cad4baf9f9c7f74819458518d24a

1

АВТНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ  
«ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ»  
«ОТКРЫТЫЙ ТАВРИЧЕСКИЙ КОЛЛЕДЖ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ  
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
(код, наименование)

ПО СПЕЦИАЛЬНОСТИ  
09.02.12 ТЕХНИЧЕСКАЯ ЭКСПЛУАТАЦИЯ И СОПРОВОЖДЕНИЕ  
ИНФОРМАЦИОННЫХ СИСТЕМ  
(код, наименование)

СПЕЦИАЛИСТ ПО ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ И  
СОПРОВОЖДЕНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ  
(квалификация)

БАЗОВЫЙ УРОВЕНЬ ПОДГОТОВКИ  
(базовый, углубленный)

ФОРМА ОБУЧЕНИЯ  
ОЧНАЯ

Симферополь, 2026г.

РАССМОТРЕНА и ОДОБРЕНА  
на заседании цикловой комиссии  
по профессиональной и практической  
подготовке специальности 09.02.12  
Техническая эксплуатация и  
сопровождение информационных  
систем.

Протокол №4 от 28.05.2026г.

Председатель цикловой комиссии  
Бридель Т. В.

Разработана на основе Федерального  
государственного образовательного  
стандарта по специальности 09.02.12  
Техническая эксплуатация и  
сопровождение информационных  
систем.

Утвержденного Приказом  
Минпросвещения России от 10 марта  
2025 года №184

(код, наименование специальности, название Приказа  
Минобра -№ и дата)

Разработчики:

Преподаватель, Сабодаш О.С.

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

**СОДЕРЖАНИЕ ПРОГРАММЫ**

<b>СОДЕРЖАНИЕ ПРОГРАММЫ.....</b>	<b>44</b>
<b>1. Общая характеристика РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....</b>	<b>45</b>
1.1. <i>Цель и место дисциплины в структуре образовательной программы.....</i>	<i>45</i>
1.2. <i>Планируемые результаты освоения дисциплины.....</i>	<i>45</i>
<b>2. Структура и содержание ДИСЦИПЛИНЫ.....</b>	<b>48</b>
2.1. <i>Трудоемкость освоения дисциплины.....</i>	<i>48</i>
2.2. <i>Содержание дисциплины.....</i>	<i>49</i>
<b>3. Условия реализации ДИСЦИПЛИНЫ.....</b>	<b>50</b>
3.1. <i>Материально-техническое обеспечение.....</i>	<i>50</i>
3.2. <i>Учебно-методическое обеспечение.....</i>	<i>50</i>
<b>4. Контроль и оценка результатов освоения ДИСЦИПЛИНЫ.....</b>	<b>51</b>

# 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.

## 1.2. Планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины обучающийся должен:

<b>Код ОК, ПК</b>	<b>Уметь</b>	<b>Знать</b>	<b>Владеть навыками</b>
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	номенклатура	-

	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	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	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.

		<p>безопасности информации и методов ее защиты.</p> <p>стандартные криптографические алгоритмы для шифрования данных</p> <p>принципы обеспечения безопасности передачи данных по сети</p> <p>основы безопасности приложений и инфраструктуры</p> <p>методы анализа на уязвимости и мониторинга безопасности</p> <p>знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений</p> <p>понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения</p> <p>знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы</p>	<p>обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS</p> <p>соблюдение законодательства и регуляций в области защиты данных</p>
--	--	---	---

## 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	32	16
Самостоятельная работа	-	-
Теория	16	
Промежуточная аттестация – диф. зач.	XX	XX
Всего	<b>32</b>	<b>16</b>

## 2.2. Примерное содержание дисциплины

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий, курсовой проект (работа)
<b>Раздел 1. Основы информационной безопасности (32 часа)</b>	
<b>Тема 1.1. Введение в информационную безопасность</b>	<b>Содержание</b>
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.2. Управление безопасностью информации</b>	<b>Содержание</b>
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.3. Криптография</b>	<b>Содержание</b>
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.
	<b>В том числе практических и лабораторных занятий</b>
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.4. Защита сетевой инфраструктуры</b>	<b>Содержание</b>
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов
	<b>В том числе практических и лабораторных занятий</b>
	Организация защиты от атак
	Организация работы VPN и межсетевого экрана
<b>Тема 1.5. Безопасность приложений</b>	<b>Содержание</b>
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.
	<b>В том числе практических и лабораторных занятий</b>
	Тестирование на проникновение и анализ уязвимостей.
<b>Тема 1.6. Защита данных</b>	<b>Содержание</b>
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным

	<b>В том числе практических и лабораторных занятий</b>
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.7. Безопасность облачных технологий</b>	<b>Содержание</b>
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности
	<b>В том числе практических и лабораторных занятий</b>
	Изучение модели облачных услуг и их безопасности
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.8. Инциденты безопасности</b>	<b>Содержание</b>
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика
	<b>В том числе практических и лабораторных занятий</b>
	Работа с инцидентами.
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.9. Социальная инженерия и человеческий фактор</b>	<b>Содержание</b>
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности
	<b>В том числе практических и лабораторных занятий</b>
	Разработка политики информационной безопасности
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Тема 1.10. Будущее информационной безопасности</b>	<b>Содержание</b>
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности
	<b>В том числе самостоятельная работа обучающихся</b> <i>Необходимость и тематика определяются образовательной организацией</i>
<b>Промежуточная аттестация</b>	
<b>Всего 32 часа</b>	

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

#### 3.1. Материально-техническое обеспечение

**Кабинет информационных технологий**

Оборудование учебного кабинета:

Рабочее место преподавателя -1шт. Посадочные места по количеству обучающихся – 10шт.

Доска классная -1шт.

Стенд информационный -5шт. Учебно-наглядные пособия. Компьютеры с лицензионным программным обеспечением

Microsoft Windows 10 Home

Microsoft Office 2010 Professional

Справочно-правовая система "ГАРАНТ"

Adobe Acrobat Reader DC

и возможностью подключения к информационно - телекоммуникационной сети «Интернет» - 10шт. Мультимедий проектор – 1шт.

### **3.2. Учебно-методическое обеспечение**

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

#### **3.2.1. Основные печатные и/или электронные 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> (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 освоённости компетенций	Методы оценки
<p><b>Знает:</b></p> <ul style="list-style-type: none"> <li>- актуальный профессиональный и социальный контекст, в котором приходится работать и жить;</li> <li>- основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;</li> <li>- алгоритмы выполнения работ в профессиональной и смежных областях;</li> <li>- методы работы в профессиональной и смежных сферах;</li> <li>- структуру плана для решения задач;</li> <li>- порядок оценки результатов решения задач профессиональной деятельности</li> <li>- номенклатуру информационных источников, применяемых в профессиональной деятельности;</li> <li>- приемы структурирования информации;</li> <li>- формат оформления результатов поиска информации, современные средства и устройства</li> </ul>	<p>Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить;</p> <p>Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте;</p> <p>Знает алгоритмы выполнения работ в профессиональной и смежных областях;</p> <p>Знает методы работы в профессиональной и смежных сферах;</p> <p>Знает структуру плана для решения задач;</p> <p>Может произвести оценку результатов решения задач профессиональной деятельности</p> <p>Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности;</p> <p>Знает приемы структурирования информации;</p> <p>Знает формат оформления результатов поиска информации, современные средства и устройства информатизации;</p> <p>Может применять</p>	<p>Экспертное наблюдение выполнения практических работ и видов работ по практике</p> <p>Диагностика (тестирование, контрольные работы)</p>

<p>информатизации;</p> <ul style="list-style-type: none"> <li>- порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;</li> <li>- лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;</li> <li>- принципы безопасности хранения данных;</li> <li>- методы защиты баз данных от внешних угроз</li> <li>- принципы криптографии и методов шифрования данных;</li> <li>- стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;</li> <li>- методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;</li> <li>- отраслевую нормативную техническую документацию и источники информации, необходимые для</li> </ul>	<p>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 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>профессиональной деятельности;</p> <ul style="list-style-type: none"> <li>- современный отечественный и зарубежный опыт в профессиональной деятельности;</li> <li>- принципы и методы обеспечения безопасности информационных систем;</li> <li>- принципы безопасности информационных систем;</li> <li>- современные методы и технологии в области безопасности информационных систем;</li> <li>- законодательные и нормативные акты в области безопасности информационных систем;</li> <li>- источники угроз информационной безопасности и меры по их предотвращению;</li> <li>- основные угрозы безопасности мобильных приложений;</li> <li>- принципы криптографии и шифрования данных;</li> <li>- стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;</li> <li>- законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA;</li> <li>- основные принципы безопасности информации и методов ее</li> </ul>	<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>защиты;</p> <ul style="list-style-type: none"> <li>- стандартные криптографические алгоритмы для шифрования данных;</li> <li>- принципы обеспечения безопасности передачи данных по сети;</li> <li>- основы безопасности приложений и инфраструктуры;</li> <li>- методы анализа на уязвимости и мониторинга безопасности;</li> <li>- знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений;</li> <li>- понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения;</li> <li>- знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.</li> </ul> <p><b>Умеет:</b></p> <ul style="list-style-type: none"> <li>-распознавать задачу и/или проблему в профессиональном и/или социальном контексте;</li> </ul>	<p>криптографические алгоритмы для шифрования данных;</p> <p>Имеет представление о принципах обеспечения безопасности передачи данных по сети;</p> <p>Знает основы безопасности приложений и инфраструктуры;</p> <p>Знает методы анализа на уязвимости и мониторинга безопасности;</p> <p>Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;</p> <p>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;</p> <p>Анализирует задачу и/или проблему и может выделить её составные части;</p> <p>Умеет определять этапы решения задачи;</p>	
--	---	--

<p>-анализировать задачу и/или проблему и выделять её составные части;</p> <p>- определять этапы решения задачи;</p> <p>- выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;</p> <p>-составлять план действия;</p> <p>- определять необходимые ресурсы;</p> <p>- владеть актуальными методами работы в профессиональной и смежных сферах;</p> <p>- реализовывать составленный план;</p> <p>- оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);</p> <p>- определять задачи для поиска информации;</p> <p>- определять необходимые источники информации;</p> <p>- планировать процесс поиска;</p> <p>- структурировать получаемую информацию; - выделять наиболее значимое в перечне информации;</p> <p>- оценивать практическую значимость результатов поиска;</p> <p>- оформлять результаты поиска, применять</p>	<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>средства информационных технологий для решения профессиональных задач;</p> <ul style="list-style-type: none"> <li>- использовать современное программное обеспечение;</li> <li>- использовать различные цифровые средства для решения профессиональных задач;</li> <li>- понимать тексты на базовые профессиональные темы;</li> <li>- шифрование данных и обеспечивает их конфиденциальность;</li> <li>- анализировать требования безопасности информационных систем;</li> <li>- разрабатывать и реализовывать меры безопасности;</li> <li>- реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.</li> </ul>	<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>	
---	---	--