

**Автономная некоммерческая организация
Профессиональная образовательная организация
«Социально-педагогический колледж» (АНО ПОО СПК)**

**«УТВЕРЖДЕНО»
Директор АНО ПОО СПК
«25» декабря 2025 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.05 «Основы информационной безопасности»

по программе подготовки специалистов среднего звена по специальности
09.02.11 «Разработка и
управление программным обеспечением»

Квалификация выпускника: Программист

МОСКВА, 2025

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.05 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, представленными в матрице компетенций выпускника (п. 4.3 ПОП).

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	номенклатура	-
	поиска информации; определять необходимые источники	информационных источников, применяемых в	

	<p>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</p>	<p>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.</p>	
ОК.03	<p>определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности, выявлять источники финансирования; презентовать идеи</p>	<p>содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности, правовой и финансовой грамотности; правила разработки презентации; основные этапы разработки и реализации проекта.</p>	
	<p>открытия собственного дела в профессиональной деятельности; определять источники достоверной правовой</p>		

	информации; составлять различные правовые документы; находить интересные проектные идеи, грамотно их формулировать и документировать; оценивать жизнеспособность проектной идеи, составлять план проекта.		
ОК.05	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке; проявлять толерантность в рабочем коллективе	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений	
ОК.09	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов 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

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах
Учебные занятия	70
Самостоятельная работа	7
Промежуточная аттестация	6
Всего	83

2.2. Содержание дисциплины

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий, курсовой проект (работа)
Раздел 1. Основы информационной безопасности	
Тема 1.1. Введение в информационную безопасность	Содержание
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>
Тема 1.2. 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.)
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>
Тема 1.3. Криптография	Содержание
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.
	В том числе практических и лабораторных занятий
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.
В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>	
Тема 1.4. Защита сетевой инфраструктуры	Содержание
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов
	В том числе практических и лабораторных занятий
	Организация защиты от атак Организация работы VPN и межсетевого экрана
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>
Тема 1.5. Безопасность приложений	Содержание
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.
	В том числе практических и лабораторных занятий Тестирование на проникновение и анализ уязвимостей.
	В том числе самостоятельная работа обучающихся

	<i>Необходимость и тематика определяются образовательной организацией</i>
Тема 1.6. Защита данных	Содержание
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным
	В том числе практических и лабораторных занятий
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным
Тема 1.7. Безопасность облачных технологий	Содержание
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности
	В том числе практических и лабораторных занятий
	Изучение модели облачных услуг и их безопасности
Тема 1.8. Инциденты безопасности	Содержание
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика
	В том числе практических и лабораторных занятий
	Работа с инцидентами.
Тема 1.9. Социальная инженерия и человеческий фактор	Содержание
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности
	В том числе практических и лабораторных занятий
	Разработка политики информационной безопасности
Тема 1.10. Будущее информационной безопасности	Содержание
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности
	В том числе самостоятельная работа обучающихся
	<i>Необходимость и тематика определяются образовательной организацией</i>
Промежуточная аттестация	
Всего 83 часа	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Наименование учебных кабинетов, лабораторий, мастерских, объектов физической культуры и спорта и других помещений с указанием перечня и количества основного оборудования

Учебная аудитория для проведения занятий лекционных, практических, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации обучающихся всех направлений подготовки, а также для самостоятельной работы.

Специализированная мебель и технические средства обучения:

- Настенная маркерная доска/экран – 1 шт.,

- Стол преподавателя – 1 шт.,
- Стул преподавателя – 1 шт.,
- Парты – 14 шт.,
- Стулья деревянные – 28 шт.,
- Шкаф книжный – 4 шт.,
- Вешалка – 1 шт.
- Переносной мобильный мультимедиа комплекс с доступом к сети Интернет:
 - Ноутбук Acer №3 Acer Aspire 5820TG (Intel Core i5 CPU M450 2,40 GHz 4 Gb)
 - Беспроводная мышь Logitech M235
 - Проектор Epson BB-X18 H551B
 - Телевизор Samsung UE42F5000AK.

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или 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 (или) 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>Знает:</p> <ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> 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; 	<ul style="list-style-type: none"> Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)
<ul style="list-style-type: none"> решения задач; - порядок оценки результатов решения задач 	<ul style="list-style-type: none"> Знает структуру плана для решения задач; Может произвести оценку 	

<p>профессиональной деятельности</p> <ul style="list-style-type: none"> - 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.; 	<p>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 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,</p>	
<ul style="list-style-type: none"> - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных 	<p>Kerberos и др.;</p> <p>Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и</p>	

<p>законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;</p> <p>- отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности;</p> <p>- современный отечественный и зарубежный опыт в профессиональной деятельности;</p> <p>- принципы и методы обеспечения безопасности информационных систем;</p> <p>- принципы безопасности информационных систем;</p> <p>- современные методы и технологии в области безопасности информационных систем;</p> <p>- законодательные и нормативные акты в области безопасности информационных систем;</p> <p>- источники угроз информационной безопасности и меры по их предотвращению;</p> <p>- основные угрозы безопасности мобильных приложений;</p> <p>- принципы криптографии</p>	<p>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>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</p>	
--	---	--

<p>и шифрования данных;</p> <ul style="list-style-type: none"> - 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; <p>- стандартные криптографические алгоритмы для шифрования данных;</p> <ul style="list-style-type: none"> - принципы обеспечения безопасности передачи данных по сети; <p>- основы безопасности приложений и инфраструктуры;</p> <ul style="list-style-type: none"> - 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 	<p>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 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</p>	
---	---	--

<p>обнаружения вторжений и антивирусные программы.</p> <p>Умеет:</p> <ul style="list-style-type: none"> -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 	<p>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>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</p>	
<p>поиска;</p> <ul style="list-style-type: none"> - оформлять результаты поиска, применять 	<p>значимое в перечне информации;</p> <p>Умеет оценивать</p>	

<p>средства информационных технологий для решения профессиональных задач;</p> <ul style="list-style-type: none"> - 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. 	<p>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 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>	
---	--	--