

ПРИЛОЖЕНИЕ 1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ

ОГЛАВЛЕНИЕ

«ПМ.01 НАИМЕНОВАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ»	2
«ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»...Ошибка! Закладка не определена.	
ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ (УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ)	Ошибка! Закладка не определена.

Рабочая программа профессионального модуля

**«ПМ.02 Защита информации в автоматизированных системах программными и
программно-аппаратными средствами»**

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Общая характеристика РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	4
1.1. <i>Цель и место профессионального модуля в структуре образовательной программы</i>	4
1.2. <i>Планируемые результаты освоения профессионального модуля</i>	4
1.3. <i>Обоснование часов вариативной части ОПОП-П.....</i>	7
2. Структура и содержание профессионального модуля	8
2.1. <i>Трудоемкость освоения модуля</i>	8
2.2. <i>Структура профессионального модуля</i>	9
2.3. <i>Содержание профессионального модуля</i>	10
2.4. <i>Курсовой проект (работа) (для специальностей СПО, если предусмотрено)</i>	20
3. Условия реализации профессионального модуля	21
3.1. <i>Материально-техническое обеспечение</i>	21
3.2. <i>Учебно-методическое обеспечение</i>	21
4. Контроль и оценка результатов освоения профессионального модуля	21

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

Профессиональный модуль включен в обязательную часть образовательной программы.

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен¹:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	-
ОК.02	Использовать современные средства поиска, анализа и	номенклатура информационных источников,	-

¹ Берутся сведения, указанные по данному виду деятельности в п. 4.2.

	интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	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.03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты	-
ОК.04	Эффективно взаимодействовать и работать в коллективе и команде	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	-
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная	-

		лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	
ПК 2.1	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	– установка, настройка программных средств защиты информации в автоматизированной системе
ПК 2.2	– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	– обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – использование программных и программно-аппаратных средств для защиты информации в сети
ПК 2.3	– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	– тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации
ПК 2.4	– применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – типовые модели управления доступом,	– решение задач защиты от НСД к информации ограниченного доступа; – применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

	доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись	средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации	
ПК 2.5	– применять средства гарантированного уничтожения информации	– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	– учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
ПК 2.6	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	– работа с подсистемами регистрации событий; – выявление событий и инцидентов безопасности в автоматизированной системе

1.3. Обоснование часов вариативной части ОПОП-П

№№ п/п	Дополнительные профессиональные компетенции	Дополнительные знания, умения, навыки	№, наименование темы	Объем часов	Обоснование включения в рабочую программу
--------	---	---------------------------------------	----------------------	-------------	---

	-	-	-	-	-
--	---	---	---	---	---

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	Объем в часах	В т.ч. в форме практической подготовки
Учебные занятия ²	360	434
Курсовая работа (проект)	40	-
Самостоятельная работа	26	-
Практика, в т.ч.:	216	216
учебная	72	72
производственная	144	144
Промежуточная аттестация, в том числе: <i>МДК 02.01 в форме экзамена</i> <i>МДК 02.02 в форме экзамена</i> <i>УП 02.01 в форме Диф. зачета</i> <i>ПП 02.01 в форме зачета</i> <i>ПМ 02 (в форме ДЭ по ПМ)</i>	24	12
Всего	588	434

² Учебные занятия на усмотрение образовательной организации могут быть разделены на теоретические занятия, лабораторные и практические занятия

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия ³	Курсовая работа (проект)	Самостоятельная работа ⁴	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8	9	10
ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9	Раздел 1. Программные и программно-аппаратные средства защиты информации	260	162	260	188	40	18		
ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9	Раздел 2. Криптографические средства защиты информации	100	44	100	84	-	8		
	Учебная практика	72	72					72	
	Производственная практика	144	144						144
	Промежуточная аттестация по ПМ	12							
	Всего:	588	322		272	40	26	X	X

³ Если в таблице 2.1. предусмотрено разделение учебных занятий на теоретические, практические и лабораторные работы, то в таблицу 2.2. должны быть добавлены соответствующие столбцы

⁴ Самостоятельная работа в рамках образовательной программы планируется образовательной организацией.

2.3. Содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятия, <i>курсовая работа (проект)</i>	Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч.	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Программные и программно-аппаратные средства защиты информации (260 часов)			
МДК 02.01 Программные и программно-аппаратные средства защиты информации		260/162	
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	30/16	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации. Основные концепции безопасности.		
	Политика информационной безопасности. Определение политики ИБ. Задачи политики ИБ. Практические шаги реализации политики ИБ. Жизненный цикл политики ИБ.		
	Сетевая политика безопасности. Шаблоны политик ИБ. Стратегические границы сети. Роль межсетевого экрана в безопасности организации. Эшелонированная оборона.		
	Управление рисками ИБ. Понятийный аппарат управления рисками. Процесс оценки рисков. Уровни вероятности и степень влияния.		
	Аудит информационной безопасности. Понятие аудита, разновидности, инструменты реализации.		
	Средства анализа защищенности АС. Примеры и особенности средств анализа отечественного и иностранного производства.		
	Kali Linux, как средство анализа защищенности АС. Особенности дистрибутива, история, инструментарий.		
	В том числе практических и лабораторных занятий		
	Практическая работа №1 Исследование корректности систем защиты		
	Практическая работа №2 Исследование систем стенографической защиты		
	Практическая работа №3 Исследование специальных систем поиска, восстановления и безвозвратного уничтожения конфиденциальных файлов		
	Практическая работа №4 Составление отчета оценки риска		

	Практическая работа №5 Исследование программ для шифрования данных на съемных носителях		
	Практическая работа № 6 Ограничение доступа на вход в систему		
	Практическая работа № 7 Идентификация и аутентификация пользователей		
	Практическая работа № 8 Разграничение доступа		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.2. Вредоносное программное обеспечение	Содержание	16/8	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Основные особенности вредоносного ПО. Определение, разновидности, способы распространения вредоносного ПО. Назначение компьютерного вируса, классификация и жизненный цикл вирусов.		
	Троянские кони. Сетевые черви. Руткиты. Особенности представителей вредоносного ПО. Отличительные черты.		
	Элементы защиты от вредоносного ПО. Принцип необнаружимости компьютерного вируса. Признаки инфицирования. Интервал возможного инфицирования. Методы обнаружения вирусов.		
	Технологии Black и Witelisteng. Назначение и отличительные особенности технологий.		
	В том числе практических и лабораторных занятий	8	
	Изучение алгоритмов известных вирусов		
	Установка антивирусной программы		
	Настройка антивирусной программы		
	Тестирование антивирусной программы		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.3. Сетевые атаки	Содержание	34/22	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Сетевые атаки. Типы и виды атак. Элементы терминологии сетевых атак.		
	Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Выбор экспойта. Взлом и загрузка груза. Соккрытие следов атаки.		
	Атаки на отказ в обслуживании. Цели атаки. Распределенная и нераспределенная атаки. Распределенные рефлекторные атаки. Таксономия атаки.		
	Примеры атак. Атака Митника. Эксплуатация UDP, TCP, IP, ICMP.		
	Классификация атак. Матричные схемы. Процессы. Классификация Ховарда. Онтология атаки.		

	Оценивание серьезности атаки. Параметр важности CERT. Показатель серьезности GIAC. Примеры вычисления.		
	В том числе практических и лабораторных занятий	22	
	Установка и первоначальная настройка средства анализа защищенности АС		
	Подготовка целевого ПК: развертывание ОС, основных сервисов		
	Подготовка целевого ПК: развертывание дополнительных сервисов		
	Использование пассивных методов анализа ИС		
	Использование активных методов анализа ИС		
	Использование сканера безопасности NMAP		
	Использование сканера безопасности Nessus		
	Использование Wireshark для анализа безопасности передачи данных		
	Спуффинг трафика		
	Анализ безопасности механизма авторизации		
	Восстановление хешей паролей		
	В том числе самостоятельная работа обучающихся		
	<i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.4. Защита информации на машинных носителях	Содержание	26/16	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Проблема защиты отчуждаемых компонентов ПЭВМ. Виды угроз для цифровой информации.		
	Методы защиты информации на отчуждаемых носителях. Основные методы защиты информации на отчуждаемых носителях.		
	Средства восстановления остаточной информации. Уровни восстановления. Применение средств восстановления остаточной информации при расследовании инцидентов.		
	Нормативная база, документирование результатов.		
	Безвозвратное удаление данных. Принципы и алгоритмы.		
	В том числе практических и лабораторных занятий	16	
	Применение средства восстановления остаточной информации на примере Foremost или аналога		
	Применение специализированного программного средства для восстановления удаленных файлов		
	Применение программ для безвозвратного удаления данных		
	Применение программ для шифрования данных на съемных носителях		
	Построение RAID массива в ОС Windows		

	Построение RAID массива в ОС Linux		
	Развертывание VPN стандартными средствами		
	Развертывание прокси-сервера (Proxy)		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.5. Защита информации от внутренних угроз информационной безопасности.	Содержание	44/26	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Обзор DLP технологий. Разновидности DLP технологий. Достоинства и недостатки технологий.		
	Введение в DLP InfoWatch Traffic Monitor. Архитектура системы. Назначение компонентов.		
	Технологии DLP InfoWatch Traffic Monitor. Особенности взаимодействия компонент.		
	Типовые сценарии применения DLP в организациях различных секторов экономики. Пример сценариев. Особенности реализации.		
	Разработка политик безопасности. Политики перекрывающих максимально возможные каналы передачи данных и возможные инциденты.		
	Проведение классификации уровня угрозы инцидента. Классы угроз, отличительные особенности.		
	Регулярные выражения. Особенности составления регулярных выражений.		
	Анализ выявленных инцидентов информационной безопасности. Методика анализа, особенности реализации.		
	Стандарт компетенции WSSS «Корпоративная защита от внутренних угроз информационной безопасности». Ознакомление с WSI и Ворлдскиллс Россия.		
	В том числе практических и лабораторных занятий	26	
	Создание и настройка виртуальных машин		
	Установка IWTM		
	Работа с AD, доменом, установка IWDM, настройка компонентов IWTM		
	Работа с AD, доменом, установка IWDM, настройка компонентов IWTM		
	«Технологии» и «Объекты защиты» в IWTM		
	«Политики» в IWTM		
	«Персоны» и «Списки» в IWTM		
	Создание тестовой политики в IWTM		

	«Категории и термины» и «Графические Объекты» в IWTM «Текстовые объекты» в IWTM «Эталонные документы», «Бланки» и «Выгрузки из БД» в IWTM Применение регулярных выражений в IWTM «Сводка» и «Отчеты» в IWTM В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 1.6 Применение программно- аппаратных средств в корпоративной системе безопасности	Содержание	26/12	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Программно-аппаратные средства защиты от НСД. Разновидности средств. Особенности применения.		
	Безопасность маршрутизаторов. Аутентификация протоколов RIPv2, OSPF, EIGRP.		
	DHCP-snooping и ARP- spoofing. Алгоритм атак. Методы защиты.		
	Защита протоколов STP. Алгоритм атак. Методы защиты.		
	Модель AAA. Компоненты модели. Особенности реализации на устройствах. Применение протокола Radius для безопасной аутентификации.		
	Технологии защиты Windows Server. Технологии защиты, реализованные в Windows Server.		
	Технологии защиты Linux. Технологии защиты, реализованные в Linux		
	В том числе практических и лабораторных занятий	12	
	Установка и настройка ПАК «Соболь»		
	Настройка аутентификации маршрутизаторов		
	Реализация защиты от DHCP-snooping и ARP- spoofing		
	Реализация защиты протоколов STP		
	Настройка локальной аутентификации		
	Настройка аутентификации с использованием Radius		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
	Тема 1.7 Мониторинг и журнализация событий в системе безопасности	Содержание	24/12
Понятие события, инцидента, алерта и журнала (лог-файла). Разница между мониторингом и аудитом.			
Классификация событий безопасности (сетевые, системные, прикладные, события доступа, изменения конфигураций).			

	Жизненный цикл события: генерация, сбор, нормализация, хранение, ротация, архивация.		
	Нормативные требования к логированию (PCI DSS, ISO 27001, ФСТЭК России, GDPR, 152-ФЗ и др.).		
	Протоколы журнализации и сбора статистики. Особенности работы и настройки протоколов Syslog и NetFlow;		
	Мониторинг событий с помощью SNMP. Особенности работы и настройки протокола SNMP		
	В том числе практических и лабораторных занятий	12	
	Настройка сбора системных логов на Linux (syslog/rsyslog). Научиться настраивать централизованный сбор логов с нескольких хостов.		
	Аудит файловой системы в Linux (auditd). Настроить отслеживание критических изменений в файлах и каталогах.		
	Установка и настройка ELK Stack (Elasticsearch, Logstash, Kibana) для сбора логов.		
	Настройка Syslog		
	Настройка NetFlow		
Настройка SNMP			
В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>			
Тема 1.8 Сетевые экраны и туннели	Содержание	16/8	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN.		
	Протоколы PPP, GRE. Структура кадра (пакета). Особенности работы и настройки.		
	Протокол IPSec: обмен ключами. Режимы работы. Протокол обмена ключами.		
	Протокол IPSec: аутентификация заголовка, безопасная инкапсуляция. Протокол аутентификации заголовка и безопасной инкапсуляции содержимого пакета.		
	В том числе практических и лабораторных занятий	8	
	Базовое фильтрование трафика на Linux (iptables/nftables). Освоить создание правил разрешающей и запрещающей политики.		

	Межсетевой экран на базе pfSense (или VyOS). Получить навыки работы с промышленным/дистрибутивным фаерволом.		
	Организация VPN-туннеля «точка-точка» (WireGuard). Настроить быстрое и безопасное соединение между двумя узлами.		
	Remote Access VPN с аутентификацией (OpenVPN). Развернуть сервер OpenVPN для удалённых сотрудников с проверкой по сертификатам или логину/пароллю.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Курсовой проект (работа)		40 / 40	
Раздел 2. Криптографические средства защиты информации			
МДК 02.02 Криптографические средства защиты информации		100 / 44	
Тема 2.1. Введение в криптографию	Содержание	2	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Предмет и задачи криптографии. Место криптографии в системе защиты информации. История развития. Основные термины. Криптосистема, требования к ней.		
Тема 2.2. Математические основы криптографии	Содержание	14 / 8	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Арифметика целых чисел. Деление, НОД, алгоритм Евклида (расширенный). Модульная арифметика, инверсии. Функция Эйлера, теоремы Эйлера и Ферма. Сравнения и их свойства. Решение сравнений первой степени. Китайская теорема об остатках. Генерация простых чисел, тесты простоты.		
	В том числе практических и лабораторных занятий	8	
	Вычисление НОД и решение диофантовых уравнений. Вычисление инверсий по модулю. Решение уравнений сравнения первой степени. Решение систем сравнений (китайская теорема). Генерация простых чисел, проверка на простоту.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 2.3. Кодирование информации	Содержание	10 / 6	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Понятие кода, равномерные и неравномерные коды. Эффективное кодирование. Дерево кода, средняя длина. Алгоритмы Шеннона-Фано и Хаффмана. Помехоустойчивое кодирование: код Хэмминга. Буквенно-цифровое кодирование.		
	В том числе практических и лабораторных занятий	6	

	Построение кодов Шеннона-Фано и Хаффмана. Кодирование и декодирование кодом Хэмминга. Буквенно-цифровое кодирование.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 2.4. Классические методы шифрования	Содержание	14 / 8	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Простейшие шифры: замены (простая, многоалфавитная, пропорциональная), перестановки (табличная, маршрутная). Гаммирование с конечной и бесконечной гаммой. Комбинирование шифров.		
	В том числе практических и лабораторных занятий	8	
	Шифрование методом замены (шифр Цезаря, Виженера). Шифрование методом перестановки. Программная реализация простейших шифров. Гаммирование (генерация гаммы, XOR).		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 2.5. Криптоанализ классических шифров	Содержание	10 / 6	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Основные методы криптоанализа. Криптографические атаки. Анализ частотности символов. Полный перебор ключей. Криптографическая стойкость, принципы Киркгоффа.		
	В том числе практических и лабораторных занятий	6	
	Криптоанализ шифра простой замены (частотный анализ). Криптоанализ шифра Виженера. Дешифрование методом перебора.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 2.6. Блочные и поточные шифры. Генераторы ПСЧ	Содержание	14 / 8	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Блочные шифры: принципы построения, сеть Фейстеля. Стандарты DES, AES, ГОСТ 28147-89 (Магма, Кузнечик). Режимы шифрования. Поточные шифры: принципы, генераторы псевдослучайных чисел (линейный конгруэнтный, VBS, Фибоначчи).		
	В том числе практических и лабораторных занятий	8	
	Исследование сети Фейстеля (программная модель). Шифрование/дешифрование с помощью алгоритма AES (OpenSSL). Реализация генератора ПСЧ и его применение для гаммирования.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
	Содержание	10 / 4	ПК 2.1-ПК 2.6

Тема 2.7. Симметричные и асимметричные криптосистемы	Симметричные системы: общая схема, отечественные и международные стандарты. Асимметричные системы: концепция открытого ключа, алгоритм RSA. Алгоритм Диффи-Хеллмана для обмена ключами.		ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	В том числе практических и лабораторных занятий	4	
	Шифрование с помощью алгоритма RSA (генерация ключей, шифрование/дешифрование). Реализация протокола Диффи-Хеллмана.		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
Тема 2.8. Хеш- функции и электронная подпись (ЭП)	Содержание	8 / 4	ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Аутентификация данных. Однонаправленные хеш-функции (MD5, SHA, ГОСТ Р 34.11-2012). Алгоритмы цифровой подписи (RSA, ГОСТ Р 34.10-2012). Применение ЭП.		
	В том числе практических и лабораторных занятий	4	
	Вычисление хешей с помощью утилит (md5sum, sha256sum). Генерация и проверка электронной подписи (например, OpenSSL)		
Тема 2.9. Компьютерная стеганография и уничтожение информации	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		ПК 2.1-ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 04, ОК 9
	Содержание	4	
	Понятие стеганографии, цифровые водяные знаки. Методы скрытой передачи информации. Гарантированное уничтожение информации (алгоритмы перезаписи).		
	В том числе самостоятельная работа обучающихся <i>Необходимость и тематика определяются образовательной организацией</i>		
В том числе самостоятельная работа обучающихся		8	
– Подготовка сравнительного обзора симметричных и асимметричных алгоритмов шифрования (стандарты, скорость, стойкость).			
– Анализ нормативных документов (ГОСТы в области криптографии).			
– Разработка простейшего шифратора/дешифратора на выбранном языке программирования			
Промежуточная аттестация по МДК.02.02 в форме Экзамена		6	
Учебная практика Виды работ: 1. криптографическое закрытие данных; 2. организация защищенного документооборота в электронных сетях; 3. криптоанализ защищенных данных; 4. предотвращение выхода конфиденциальных данных за периметр организации;		72	

5. документирование и презентация решений.		
Производственная практика Виды работ: 1. анализ принципов построения систем информационной защиты производственных подразделений; 2. техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы; 3. участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; 4. анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении; 5. участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; 6. применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	144	
Промежуточная аттестация по ПМ	12	
Всего	588	

2.4. Курсовой проект (работа) (для специальностей СПО, если предусмотрено)

Выполнение курсового проекта по модулю — обязательное условие, при котором обучающийся может выбрать тему в рамках текущего модуля, смежного профессионального модуля.

Тематика курсовых проектов (работ)

1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
5. Проблема защиты информации в облачных хранилищах данных и ЦОДах
6. Защита сред виртуализации

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Лаборатория Лаборатория инженерно-технических средств обеспечения информационной безопасности, оснащенная в соответствии с приложением 3 ПОП.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Введение в теоретико-числовые методы криптографии: учебное пособие для СПО / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/265178>

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт. — URL: <https://urait.ru/bcode/518005>

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

4. Прохорова, О. В. Информационная безопасность и защита информации: учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4.

3.2.2. Дополнительные источники *(при необходимости)*

1. ГОСТ Р 59381-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции».

2. ГОСТ ISO/IEC 24760-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования».

3. ГОСТ Р 59382-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы».

4. ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом».

5. ГОСТ ISO/IEC 27014-2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности».

6. ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных».

7. ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».

8. ГОСТ Р 59503-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации».

9. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».

10. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».

11. ГОСТ Р 59515-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности».

12. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

13. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».

14. ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации».

15. ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

16. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

17. ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей».

18. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».

19. ГОСТ Р ИСО/МЭК 27033-4-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности».

20. ГОСТ Р ИСО/МЭК 27033-5-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)».

21. ГОСТ Р 59162-2020 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей».

22. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

23. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

24. ГОСТ Р 34.12-2015 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».

25. ГОСТ 34.12-2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».

26. ГОСТ Р 34.13-2015 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».

27. ГОСТ 34.13-2018 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».

28. ГОСТ Р 34.10-2012 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

29. ГОСТ 34.10-2018 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

30. ГОСТ Р 34.11-2012 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».

31. ГОСТ 34.11-2018 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоённости компетенций)	Формы контроля и методы оценки ⁵
ПК 2.1	Выполняет установку отдельных программных, программно-аппаратных средств защиты информации; Настраивает отдельные программные, программно-аппаратные средства защиты информации	Контрольные работы, зачеты, квалификационные испытания, учебная и производственная практики, экзамены. Интерпретация результатов выполнения практических/ лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.
ПК 2.2	Обеспечивает защиту информации в автоматизированных системах отдельными программными средствами; Обеспечивает защиту информации в автоматизированных системах отдельными программно-аппаратными средствами	
ПК 2.3	Выполняет перечень работ по тестированию функций отдельных программных средств защиты информации; Выполняет перечень работ по тестированию функций отдельных программно-аппаратных средств защиты информации	
ПК 2.4	Обрабатывает и хранит информацию ограниченного доступа; Передаёт информацию ограниченного доступа	
ПК 2.5	Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных средств; Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программно-аппаратных средств	
ОК.01	распознаёт задачу и/или проблему в профессиональном и/или социальном контексте; анализирует задачу и/или проблему; определяет этапы решения задачи; выявляет и эффективно находит информацию, необходимую для решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; оценивает результат и последствия своих действий (самостоятельно или с помощью наставника)	
ОК.02	определяет задачи для поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует	

⁵ Примеры оформления формы контроля: контрольные работы, зачеты, квалификационные испытания, защита курсовых и дипломных проектов (работ), экзамены. Примеры оформления методов оценки: интерпретация результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.

	полученную информацию; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; оформляет результаты поиска	
ОК.03	определяет актуальность нормативно-правовой документации в профессиональной деятельности; применяет современную научную профессиональную терминологию; определяет и выстраивает траектории профессионального развития и самообразования	
ОК.04	организовывает работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности	
ОК.05	излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе	
ОК.06	описывает значимость своей специальности	
ОК.07	соблюдает нормы экологической безопасности определять направления ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК.08	чередует смену деятельности; выполняет комплекс лечебной гимнастики с учетом профессиональной деятельности	
ОК.09	понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы; пишет простые связные сообщения на знакомые или интересующие профессиональные темы	

ПРИЛОЖЕНИЕ 1.1.1.1
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

УП.02.01 ПМ.02 Защита информации в автоматизированных системах
программными и программно-аппаратными средствами

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	28
1.2. Планируемые результаты освоения учебной практики.....	29
1.3. Обоснование часов учебной практики в рамках вариативной части ОПОП-П.....	Ошибка! Закладка не определена.
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	30
2.1. Трудоемкость освоения учебной практики	30
2.2. Структура учебной практики	30
2.3. Содержание учебной практики.....	32
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ...	36
3.1. Материально-техническое обеспечение учебной практики	36
3.2. Учебно-методическое обеспечение	36
3.3. Общие требования к организации учебной практики.....	37
3.4 Кадровое обеспечение процесса учебной практики.....	37
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	38

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Цель и место учебной практики в структуре образовательной программы:

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности *10.02.05 Обеспечение информационной безопасности автоматизированных систем* и реализуется в профессиональном цикле после прохождения междисциплинарных курсов (МДК 02.01, МДК 02.02) в рамках профессиональных модулей в соответствии с учебным планом (п. 5.1. ОПОП-П):

<i>УП 02.01 Учебная практика</i>	<i>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</i>	<i>МДК.02.01 Программные и программно-аппаратные средства защиты информации</i> <i>МДК.02.02 Криптографические средства защиты информации</i>
----------------------------------	---	--

Учебная практика направлена на развитие общих (ОК) и профессиональных компетенций (ПК):

Код ОК / ПК	Наименование ОК / ПК
ОК.01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК.02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК.03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК.04	Эффективно взаимодействовать и работать в коллективе и команде
ОК.05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК.06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК.07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК.08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Цель учебной практики: формирование первоначальных практических профессиональных умений в рамках профессиональных модулей данной ОПОП-П по видам деятельности: «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1.2. Планируемые результаты освоения учебной практики

В результате прохождения учебной практики по видам деятельности, предусмотренным ФГОС СПО, обучающийся должен получить практический опыт (сформировать умения):

Наименование вида деятельности	Практический опыт / умения
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПО 1 установки, настройки программных средств защиты информации в автоматизированной системе ПО 4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации ПО 5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных ПО 6 учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности ПО 8 выявления событий и инцидентов безопасности в автоматизированной системе
	У1. производить установку и адаптацию программных средств защиты информации в автоматизированной системе У2. выполнять работы по обеспечению защиты автономных автоматизированных систем программными и программно-аппаратными средствами

	У3. участвовать в тестировании и диагностике программных и программно-аппаратных средств защиты информации У4. устранять отказы и восстанавливает работоспособность программных и программно-аппаратных средств защиты информации программирования. У5. выполнять перечень работ по решению задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации У6. осуществлять применение электронной подписи. У7. ведет учет информации, для которой установлен режим конфиденциальности У8. демонстрировать алгоритм выявления события и инцидентов безопасности в автоматизированной системе
--	--

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

2.1. Трудоемкость освоения учебной практики

Код УП	Объем, ак.ч.	Форма проведения учебной практики (концентрированно/ рассредоточено)	Курс / семестр	Форма промежуточной аттестации
УП. 02.01	36	Концентрированно	3/6	Диф.зач
УП. 02.01	36	Концентрированно	4/7	Диф.зач
Всего УП	72			

2.2. Структура учебной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем учебной практики	Объем часов
УП 02.01. ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				
ПК 2.1, ПК 2.2, ПК 2.5	Раздел 1. Защита автономных автоматизированных систем	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	Тема 1.1. Поиск следов активности вредоносного ПО	6
			Тема 1.2. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	6
		Оценка эффективности применяемых программно-аппаратных средств обеспечения	Тема 1.3. Защитные механизмы в современном программном обеспечении.	6

		информационной безопасности	Технические и юридические средства защиты.	
		Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	Тема 1.4. Защита информации от несанкционированного копирования с использованием специализированных программных средств	6
		Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	Тема 1.5. Применение средства восстановления остаточной информации на примере Foremost	6
		Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	Тема 1.6. Построение RAID массива	6
ВСЕГО ПО РАЗДЕЛУ 1				36
ПК 2.1, ПК 2.3, ПК 2.5	Раздел 2. Защита информации в информационных системах	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	Тема 2.1. Сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR	6
			Тема 2.2. Проведение аудита ЛВС сетевым сканером	6
		Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	Тема 2.3. Составление схемы защиты	6
			Тема 2.4. Внедрение защитных средств	6
		Применение программных и программно-аппаратных средств обеспечения информационной безопасности в	Тема 2.5. Установка и настройка комплексного средства на примере SecretNetStudio	6
			Тема 2.6. Установка и настройка программных средств оценки	6

		автоматизированных системах	защищенности и аудита информационной безопасности.	
ВСЕГО ПО РАЗДЕЛУ 2				36
Итого				72

2.3. Содержание учебной практики

Наименование разделов профессионального модуля и тем учебной практики	Содержание работ	Объем, ак.ч.
УП 02.01. ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами		
Раздел 1. Защита автономных автоматизированных систем		36
Тема 1.1. Поиск следов активности вредоносного ПО	Содержание	6
	Анализ типовых артефактов вредоносного ПО (процессы, автозагрузка, службы, задачи планировщика). Использование встроенных средств ОС (Task Manager, netstat, wmic) для выявления подозрительной активности. Применение утилит Sysinternals (Autoruns, Process Explorer) для обнаружения следов ВПО. Анализ журналов событий Windows (Event Viewer) на предмет несанкционированных действий. Сканирование системы антивирусными сканерами (Kaspersky Virus Removal Tool, Dr.Web CureIt) и анализ отчетов. Составление отчёта о найденных следах с указанием методов обнаружения.	
Тема 1.2. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	Содержание	6
	Изучение ключей реестра, часто используемых при закреплении ВПО (Run, RunOnce, Winlogon, Services). Практика работы с редактором реестра (regedit) и экспорт/импорт веток. Использование утилит Regshot и RegRipper для сравнения снимков реестра. Поиск следов выполнения программ по записям UserAssist, MUICache, ShimCache. Анализ веток с информацией о сетевых подключениях и открытых портах. Автоматизация поиска типовых индикаторов компрометации с помощью PowerShell-скриптов.	
	Содержание	6

Тема 1.3. Защитные механизмы в современном программном обеспечении. Технические и юридические средства защиты.	Обзор технических механизмов защиты: антивирусные движки, HIPS, межсетевые экраны (брандмауэры). Настройка встроенных защитных механизмов ОС (UAC, DEP, ASLR, Control Flow Guard). Изучение политик AppLocker и ограничений запуска приложений. Применение средств шифрования данных (BitLocker, VeraCrypt) для защиты файлов и томов. Анализ юридических средств: лицензирование, соответствие 152-ФЗ, требования к защите информации. Разработка политики безопасности для автоматизированной системы на основе технических и правовых мер.	
Тема 1.4. Защита информации от несанкционированного копирования с использованием специализированных программных средств	Содержание Изучение методов защиты от копирования: аппаратные ключи (HASP, Sentinel), лицензионные файлы, активация через сервер. Настройка защиты исполняемых файлов с помощью обфускации и упаковщиков (UPX, Themida — демо-режим). Практика использования средств DRM для документов (Adobe DRM, цифровые водяные знаки). Конфигурирование прав доступа к файлам и папкам (NTFS, EFS) для предотвращения копирования неуполномоченными пользователями. Проверка эффективности защиты: попытка копирования защищённых файлов с последующим анализом блокировок. Оформление отчёта с рекомендациями по выбору программных средств защиты от копирования.	6
Тема 1.5. Применение средства восстановления остаточной информации на примере Foremost	Содержание Установка и подготовка среды (Linux или виртуальная машина) для работы с Foremost. Создание тестового образа диска с удалёнными файлами (фотографии, документы, архивы). Изучение конфигурационного файла foremost.conf (типы файлов, заголовки, сигнатуры). Практика восстановления файлов с образа диска с использованием различных параметров (глубокий поиск, ограничение по размеру). Сравнение результатов восстановления до и после перезаписи данных. Анализ ограничений метода и составление	6

	инструкции по применению Foremost для расследования инцидентов.	
Тема 1.6. Построение RAID массива	Содержание Изучение уровней RAID (0, 1, 5, 10) и их характеристик (надёжность, производительность, отказоустойчивость). Создание программного RAID в ОС Windows (Дисковые пространства / Storage Spaces). Построение программного RAID в Linux с помощью mdadm (сборка, настройка, форматирование). Моделирование выхода из строя одного диска и восстановление массива (hot spare, rebuild). Сравнение производительности RAID 0, 1 и 5 с помощью тестов (CrystalDiskMark, dd). Оформление отчёта с выбором оптимального уровня RAID для разных сценариев использования (база данных, сервер файлов, видеонаблюдение).	6
Раздел 2. Защита информации в информационных системах		36
Тема 2.1. Сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR	Содержание Изучение архитектуры и принципов работы систем обнаружения вторжений (NIDS). Установка и настройка SNORT (правила, логирование, режимы работы). Ознакомление с возможностями RealSecure (Policy Manager, консоль событий). Анализ функционала NFR (Network Flight Recorder) и его механизмов анализа трафика. Проведение тестовых атак (сканирование портов, подбор паролей) и сравнение реакции мониторов. Составление сравнительной таблицы по критериям: производительность, гибкость правил, удобство отчётности.	6
Тема 2.2. Проведение аудита ЛВС сетевым сканером	Содержание Выбор сетевого сканера (Nmap, XSpider, MaxPatrol – ознакомительная версия). Сканирование локальной сети с определением активных хостов, открытых портов и служб. Проведение анализа уязвимостей с использованием скриптов (NSE для Nmap). Выявление сетевых ресурсов с анонимным доступом и слабых паролей. Оценка соответствия конфигурации сетевых устройств политике безопасности. Формирование отчёта по результатам аудита с перечнем рекомендаций по устранению недостатков.	6
	Содержание	6

Тема 2.3. Составление схемы защиты	Анализ структуры и топологии защищаемой информационной системы. Определение угроз и модели нарушителя для заданного сценария. Выбор необходимых средств защиты (межсетевые экраны, COB, антивирусы, VPN, IDS/IPS). Разработка схемы разграничения сетевых сегментов (DMZ, внутренняя сеть, управляющий сегмент). Нанесение на схему точек контроля и размещения средств защиты. Оформление пояснительной записки и схемы защиты с использованием MS Visio или draw.io.	
Тема 2.4. Внедрение защитных средств	Содержание Планирование поэтапного внедрения выбранных средств защиты. Установка и базовая настройка межсетевого экрана (например, iptables на Linux или pfSense). Настройка правил фильтрации трафика и трансляции адресов (NAT). Интеграция антивирусной защиты на сетевых узлах и почтовых серверах. Проверка работоспособности системы после внедрения (отсутствие блокировки легитимного трафика). Документирование выполненных работ и создание инструкции для администратора.	6
Тема 2.5. Установка и настройка комплексного средства на примере SecretNetStudio	Содержание Установка SecretNetStudio в лабораторной среде (виртуальные машины). Изучение архитектуры и компонентов системы (агенты, сервер политик, консоль управления). Настройка политик информационной безопасности: контроль доступа к файлам и устройствам. Конфигурирование межсетевого экрана и системы обнаружения вторжений в составе SecretNetStudio. Реализация защиты от утечек (DLP-функции) и контроль съёмных носителей. Тестирование работы комплекса на типовых угрозах и формирование отчёта о настройках.	6
Тема 2.6. Установка и настройка программных средств оценки защищённости и аудита информационной безопасности.	Содержание Обзор средств оценки защищённости (MaxPatrol OW, Nessus, OpenVAS, Кобра, Security Master).	6

	Установка и первоначальная настройка выбранного средства (например, OpenVAS на Kali Linux). Проведение сканирования тестовой инфраструктуры на уязвимости и ошибки конфигурации. Анализ полученных отчётов и классификация уязвимостей по степени критичности. Проведение аудита политик безопасности с использованием средств автоматизированного контроля. Разработка плана устранения выявленных уязвимостей и повторный аудит для проверки исправлений.	
Промежуточная аттестация в форме: Дифференцированного зачета		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение учебной практики

Лаборатория «Инженерно-технических средств защиты информации», оснащенная в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики (мастерские/зоны по видам работ), оснащенная(ые) в соответствии с приложением 3 ОПОП-П.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2023.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2024.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2023. – 184 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2022. – 336с

3.2.2. Дополнительные источники (при необходимости)

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

3.3. Общие требования к организации учебной практики

Учебная практика проводится в учебно-производственных мастерских, лабораториях и иных структурных подразделениях образовательного учреждения, либо в организациях в специально оборудованных помещениях на основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля (далее – Профильная организация), и образовательным учреждением.

Сроки проведения учебной практики устанавливаются образовательной организацией в соответствии с ОПОП-П по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Учебная практика реализуется в форме практической подготовки и проводится *как непрерывно, так и путем чередования с теоретическими занятиями по дням (неделям)* при условии обеспечения связи между теоретическим обучением и содержанием практики.

3.4 Кадровое обеспечение процесса учебной практики

Учебная практика проводится мастерами производственного обучения и (или) преподавателями дисциплин профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Индекс УП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
УП 02.01	ПК 2.1	ПК 2.1.1 Демонстрирует умения и практические навыки в установке отдельных программных, программно-аппаратных средств защиты информации ПК 2.1.2 Демонстрирует умения и практические навыки в настройке отдельных программных, программно-аппаратных средств защиты информации	Наблюдение, оценка выполнения заданий учебной практики, дифференцированный зачёт.
	ПК 2.2	ПК 2.2.1 Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными средствами ПК 2.2.2 Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программно-аппаратными средствами	Наблюдение, оценка выполнения заданий учебной практики, дифференцированный зачёт.
	ПК 2.3	ПК 2.3.1 Выполняет перечень работ по тестированию функций отдельных программных средств защиты информации ПК 2.3.2 Выполняет перечень работ по тестированию функций отдельных программно-аппаратных средств защиты информации	Наблюдение, оценка выполнения заданий учебной практики, дифференцированный зачёт.
	ПК 2.4	ПК 2.4.1 Обрабатывает и хранит информацию ограниченного доступа ПК 2.4.2 Передает информацию ограниченного доступа	Наблюдение, оценка выполнения заданий учебной практики, дифференцированный зачёт.
	ПК 2.5	ПК 2.5.1 Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных средств ПК 2.5.2 Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программно-аппаратных средств	Наблюдение, оценка выполнения заданий учебной практики, дифференцированный зачёт.
	ОК.01	распознает задачу и/или проблему в профессиональном и/или социальном контексте; анализирует задачу и/или проблему; определяет этапы решения	Интерпретация результатов наблюдений за деятельностью

		задачи; выявляет и эффективно находит информацию, необходимую для решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; оценивает результат и последствия своих действий (самостоятельно или с помощью наставника)	обучающегося в процессе практики.
	ОК.02	определяет задачи для поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует полученную информацию; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; оформляет результаты поиска	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.03	определяет актуальность нормативно-правовой документации в профессиональной деятельности; применяет современную научную профессиональную терминологию; определяет и выстраивает траектории профессионального развития и самообразования	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.04	организовывает работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.05	излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке, проявляет толерантность в рабочем коллективе	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.06	описывает значимость своей специальности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.07	соблюдает нормы экологической безопасности определять направления ресурсосбережения в рамках профессиональной деятельности по специальности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.08	чередует смену деятельности; выполняет комплекс лечебной гимнастики с учетом профессиональной деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.09	понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы участвовать в диалогах на знакомые общие и профессиональные темы; пишет простые связные сообщения на знакомые или	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.

		интересующие профессиональные темы	
--	--	------------------------------------	--

ПРИЛОЖЕНИЕ 1.1.1.2
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

**ПП.02 ПМ.02 Защита информации в автоматизированных системах
программными и программно-аппаратными средствами**

2026г.

СОДЕРЖАНИЕ

1.1. Цель и место учебной практики в структуре образовательной программы:	28
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	43
1.1. Цель и место производственной практики в структуре образовательной программы:	43
1.2. Планируемые результаты освоения учебной практики	44
1.3. Обоснование часов производственной практики в рамках вариативной части ОПОП-П	45
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	45
2.1. Трудоемкость освоения производственной практики	45
2.2. Структура производственной практики	45
2.3. Содержание производственной практики	47
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	55
3.1. Материально-техническое обеспечение производственной практики	55
3.2. Учебно-методическое обеспечение	55
3.3. Общие требования к организации производственной практики	56
3.4 Кадровое обеспечение процесса производственной практики	56
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	57

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Цель и место производственной практики в структуре образовательной программы:

Рабочая программа производственной практики (ПП) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем реализуется в профессиональном цикле после прохождения междисциплинарных курсов (МДК) в рамках профессиональных модулей в соответствии с учебным планом (п. 5.1. ОПОП-П):

<i>ПП 02 Производственная практика</i>	<i>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</i>	<i>МДК.02.01 Программные и программно-аппаратные средства защиты информации</i> <i>МДК.02.02 Криптографические средства защиты информации</i>
--	---	--

Производственная практика направлена на развитие общих (ОК) и профессиональных компетенций (ПК):

Код ОК / ПК	Наименование ОК / ПК
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Цель производственной практики: приобретение практического опыта в рамках профессиональных модулей данной ОПОП-П по видам деятельности: «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1.2. Планируемые результаты освоения учебной практики

В результате прохождения производственной практики по видам деятельности, предусмотренным ФГОС СПО, обучающийся должен получить практический опыт:

Наименование вида деятельности	Практический опыт / умения
Разработка и интеграция модулей программного обеспечения	ПО1. установки, настройки программных средств защиты информации в автоматизированной системе я; ПО2. обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; ПО3. тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; ПО4. решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; ПО5. применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных ПО7. учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; ПО8. работы с подсистемами регистрации событий;

	ПО9. выявления событий и инцидентов безопасности в автоматизированной системе.
	У1. производить установку и адаптацию программных средств защиты информации в автоматизированной системе У2. выполнять работы по обеспечению защиты автономных автоматизированных систем программными и программно-аппаратными средствами У3. участвовать в тестировании и диагностике программных и программно-аппаратных средств защиты информации У4. устранять отказы и восстанавливает работоспособность программных и программно-аппаратных средств защиты информации программирования. У5. выполнять перечень работ по решению задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации У6. осуществлять применение электронной подписи. У7. ведет учет информации, для которой установлен режим конфиденциальности У8. демонстрировать алгоритм выявления события и инцидентов безопасности в автоматизированной системе

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1. Трудоемкость освоения производственной практики

Код ПП	Объем, ак.ч.	Форма проведения производственной практики (концентрированно/ рассредоточено)	Курс / семестр
ПП.02.01	144	концентрированно	7
Всего ПП	144	концентрированно	7

2.2. Структура производственной практики

Код ПК	Наименование разделов профессионального модуля	Виды работ	Наименование тем производственной практики	Объем часов
ПП 02.01. ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами				
ПК 2.1, ПК 2.2, ПК 2.5	Раздел 1. Защита автономных автоматизированных систем	техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	Тема 1.1. Поиск следов активности вредоносного ПО	6
			Тема 1.2. Применение средств исследования реестра Windows для поиска следов ВПО	6

		анализ принципов построения систем информационной защиты производственных подразделений	Тема 1.3. Защитные механизмы в ПО: технические и юридические средства	6
		участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	Тема 1.4. Защита информации от несанкционированного копирования	6
			Тема 1.5. Применение средства восстановления остаточной информации (Foremost)	6
		техническая эксплуатация элементов программной и аппаратной защиты	Тема 1.6. Построение RAID-массива	6
			Тема 1.7. Оценка эффективности средств защиты автономной АС	6
		применение нормативных правовых актов, нормативных методических документов по ИБ	Тема 1.8. Разработка политики ИБ для автономной системы	6
ВСЕГО ПО РАЗДЕЛУ 1				48
ПК 2.1, ПК 2.3, ПК 2.5	Раздел 2. Защита информации в информационных (сетевых) системах	анализ принципов построения систем информационной защиты производственных подразделений	Тема 2.1. Сравнительный анализ сетевых мониторов (RealSecure, SNORT, NFR)	6
		техническая эксплуатация элементов программной и аппаратной защиты	Тема 2.2. Проведение аудита ЛВС сетевым сканером	6
		анализ эффективности применяемых программно-аппаратных средств ИБ	Тема 2.3. Составление схемы защиты	12
		участие в диагностировании, устранении отказов и обеспечении работоспособности средств ИБ	Тема 2.4. Внедрение защитных средств	6
		участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	Тема 2.5. Установка и настройка комплексного средства SecretNetStudio	12
		применение нормативных правовых актов, нормативных методических документов по ИБ	Тема 2.6. Установка и настройка средств оценки защищенности и аудита ИБ	6

ВСЕГО ПО РАЗДЕЛУ 2				48
ПК 2.4, ПК 2.5	Раздел 3. Обеспечение непрерывности и управление инцидентами ИБ	техническая эксплуатация элементов программной и аппаратной защиты участие в диагностировании, устранении отказов и обеспечении работоспособности средств ИБ	Тема 3.1. Резервное копирование и восстановление данных	12
		анализ принципов построения систем информационной защиты применение нормативных правовых актов, нормативных методических документов по ИБ	Тема 3.2. Управление инцидентами ИБ и анализ журналов событий	12
		участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	Тема 3.3. Организация защищенного удаленного доступа (VPN)	6
		анализ эффективности применяемых программно-аппаратных средств ИБ	Тема 3.4. Анализ защищенности веб-приложений	6
		применение нормативных правовых актов, нормативных методических документов по ИБ	Тема 3.5. Разработка плана реагирования на инциденты	6
		анализ эффективности применяемых программно-аппаратных средств ИБ	Тема 3.6. Аудит безопасности автоматизированной системы	6
ВСЕГО ПО РАЗДЕЛУ 3				48

2.3. Содержание производственной практики

Наименование разделов профессионального модуля и тем производственной практики	Содержание работ	Объем, ак.ч.
ПП 02.01. ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами		
Раздел 1. Защита автономных автоматизированных систем		
Тема 1.1 Поиск следов активности вредоносного ПО	Содержание	6
	Анализ типовых артефактов вредоносного ПО на автономной рабочей станции.	

	Использование встроенных средств ОС (Task Manager, netstat, wmic) для выявления подозрительной активности. Применение утилит Sysinternals (Autoruns, Process Explorer) для обнаружения следов ВПО. Анализ журналов событий Windows (Event Viewer) на предмет несанкционированных действий. Сканирование системы антивирусными сканерами (Kaspersky Virus Removal Tool, Dr.Web CureIt) и анализ отчётов. Составление отчёта о найденных следах с указанием методов обнаружения и рекомендаций по устранению.	
Тема 1.2. Применение средств исследования реестра Windows для поиска следов ВПО	Содержание	6
	Изучение ключей реестра, используемых для закрепления ВПО (Run, RunOnce, Winlogon, Services). Практика работы с редактором реестра (regedit), экспорт/импорт веток. Использование утилит Regshot и RegRipper для сравнения снимков реестра до и после заражения. Поиск следов выполнения программ по записям UserAssist, MUICache, ShimCache. Анализ веток с информацией о сетевых подключениях и открытых портах. Автоматизация поиска типовых индикаторов компрометации с помощью PowerShell-скриптов. Документирование результатов и формирование шаблона для расследования инцидентов.	
Тема 1.3 Защитные механизмы в ПО: технические и юридические средства	Содержание	6
	Обзор технических механизмов защиты: антивирусные движки, HIPS, межсетевые экраны, контроль целостности. Настройка встроенных защитных механизмов ОС (UAC, DEP, ASLR, Control Flow Guard). Изучение и применение политик AppLocker и ограничений запуска приложений. Применение средств шифрования данных (BitLocker, VeraCrypt) для защиты файлов и томов на автономной АС. Анализ юридических средств: лицензирование, соответствие 152-ФЗ, требования к защите информации. Разработка политики безопасности для автономной автоматизированной системы на основе технических и правовых мер.	
Тема 1.4 Защита информации от несанкционированного копирования	Содержание	6
	Изучение методов защиты от копирования: аппаратные ключи (HASP, Sentinel), лицензионные файлы, активация через сервер.	

	Настройка защиты исполняемых файлов с помощью обфускации и упаковщиков (UPX, Themida – демо-режим). Практика использования средств DRM для документов (Adobe DRM, цифровые водяные знаки). Конфигурирование прав доступа к файлам и папкам (NTFS, EFS) для предотвращения копирования неуполномоченными пользователями. Проверка эффективности защиты: попытка копирования защищённых файлов с последующим анализом блокировок. Оформление отчёта с рекомендациями по выбору программных средств защиты от копирования для конкретной АС.	
Тема 1.5 Применение средства восстановления остаточной информации (Foremost)	Содержание Установка и подготовка среды (Linux или виртуальная машина) для работы с Foremost. Создание тестового образа диска с удалёнными файлами (фотографии, документы, архивы). Изучение конфигурационного файла foremost.conf (типы файлов, заголовки, сигнатуры). Практика восстановления файлов с образа диска с использованием различных параметров (глубокий поиск, ограничение по размеру). Сравнение результатов восстановления до и после перезаписи данных. Анализ ограничений метода и составление инструкции по применению Foremost для расследования инцидентов в производственной среде	6
Тема 1.6 Построение RAID-массива	Содержание Изучение уровней RAID (0, 1, 5, 10) и их характеристик (надёжность, производительность, отказоустойчивость). Создание программного RAID в ОС Windows (Дисковые пространства / Storage Spaces). Построение программного RAID в Linux с помощью mdadm (сборка, настройка, форматирование). Моделирование выхода из строя одного диска и восстановление массива (hot spare, rebuild). Сравнение производительности RAID 0, 1 и 5 с помощью тестов (CrystalDiskMark, dd). Оформление отчёта с выбором оптимального уровня RAID для разных сценариев использования (база данных, сервер файлов, видеонаблюдение).	6
Тема 1.7 Оценка эффективности средств защиты автономной АС	Содержание Разработка критериев эффективности для средств защиты автономной АС (частота ложных срабатываний, нагрузка на систему, полнота обнаружения).	6

	Проведение тестовых атак (в лабораторной среде) и оценка реакции антивируса, межсетевого экрана, системы контроля целостности. Измерение производительности АС до и после внедрения средств защиты с помощью бенчмарков. Анализ журналов событий и составление отчёта о пропущенных или заблокированных угрозах. Расчёт экономической эффективности (стоимость владения, предотвращённый ущерб) для малого предприятия. Формирование итогового заключения о целесообразности применения выбранного набора средств.	
Тема 1.8 Разработка политики ИБ для автономной системы	Содержание	6
	Анализ угроз для автономной АС на основе модели нарушителя (внутренний/внешний, уровень подготовки). Изучение нормативных документов (ГОСТ, 152-ФЗ, приказы ФСТЭК) применительно к автономной системе. Разработка организационно-распорядительной документации: перечень мер, ответственные лица, порядок действий. Создание матрицы доступа и правил разграничения прав пользователей. Оформление политики безопасности в виде текстового документа и презентации. Защита разработанной политики перед руководителем практики (обоснование выбора мер).	
Раздел 2. Защита информации в информационных (сетевых) системах		
Тема 2.1. Сравнительный анализ сетевых мониторов (RealSecure, SNORT, NFR)	Содержание	6
	Изучение архитектуры и принципов работы систем обнаружения вторжений (NIDS) на примере RealSecure, SNORT, NFR. Установка и базовая настройка SNORT (правила, логирование, режимы работы). Ознакомление с возможностями RealSecure (Policy Manager, консоль событий). Анализ функционала NFR (Network Flight Recorder) и его механизмов анализа трафика. Проведение тестовых атак (сканирование портов, подбор паролей, DoS) и сравнение реакции мониторов. Составление итогового отчёта со сравнительной таблицей по критериям: производительность, гибкость правил, удобство отчётности, стоимость.	
Тема 2.2. Проведение аудита ЛВС сетевым сканером	Содержание	
	Выбор сетевого сканера для аудита ЛВС (Nmap, XSpider, MaxPatrol, OpenVAS). Сканирование локальной сети с определением	

	активных хостов, открытых портов и служб. Проведение анализа уязвимостей с использованием скриптов (NSE для Nmap). Выявление сетевых ресурсов с анонимным доступом, слабых паролей и устаревшего ПО. Оценка соответствия конфигурации сетевых устройств (коммутаторы, маршрутизаторы) политике безопасности. Формирование детализированного отчёта с перечнем уязвимостей, их критичностью и рекомендациями по устранению.	
Тема 2.3. Составление схемы защиты	Содержание	6
	Анализ топологии и структуры корпоративной информационной системы (по заданию руководителя). Определение актуальных угроз и модели нарушителя для данного сегмента сети. Выбор необходимых средств защиты: межсетевые экраны, COB, антивирусы, VPN, DLP-системы. Разработка схемы разграничения сетевых сегментов (DMZ, внутренняя сеть, управляющий сегмент). Нанесение на схему точек контроля и размещения средств защиты с обоснованием. Оформление пояснительной записки и итоговой схемы с использованием MS Visio или draw.io.	
Тема 2.4. Внедрение защитных средств	Содержание	6
	Планирование поэтапного внедрения выбранных средств защиты в действующую информационную систему. Установка и базовая настройка межсетевого экрана (iptables на Linux, pfSense, либо корпоративный Firewall). Настройка правил фильтрации трафика, трансляции адресов (NAT) и ограничений по времени. Интеграция антивирусной защиты на сетевых узлах и почтовых серверах. Проверка работоспособности системы после внедрения (отсутствие блокировки легитимного трафика). Документирование внесённых изменений и создание инструкции для администратора безопасности.	
Тема 2.5. Установка и настройка комплексного средства SecretNetStudio	Содержание	6
	Установка SecretNetStudio в лабораторной среде (несколько виртуальных машин). Изучение архитектуры и компонентов системы (агенты, сервер политик, консоль управления). Настройка политик информационной безопасности: контроль доступа к файлам, устройствам и портам. Конфигурирование встроенного межсетевого экрана и системы обнаружения вторжений.	

	Реализация защиты от утечек (DLP-функции) и контроль съёмных носителей. Тестирование комплекса на типовых угрозах (например, попытка копирования конфиденциальных данных) и формирование отчёта.	
Тема 2.6. Установка и настройка средств оценки защищённости и аудита ИБ	Содержание	6
	Обзор средств оценки защищённости и аудита ИБ (MaxPatrol OW, Nessus, OpenVAS, Кобра, Security Master). Установка и первоначальная настройка выбранного средства (например, OpenVAS на Kali Linux). Проведение сканирования тестовой инфраструктуры на уязвимости и ошибки конфигурации. Анализ полученных отчётов и классификация уязвимостей по степени критичности (CVSS). Проведение аудита политик безопасности с использованием средств автоматизированного контроля. Разработка плана устранения выявленных уязвимостей и повторный аудит для проверки исправлений.	
Раздел 3. Обеспечение непрерывности и управление инцидентами ИБ		
Тема 3.1. Резервное копирование и восстановление данных	Содержание	12
	Анализ требований к резервному копированию (RPO, RTO) для заданной информационной системы. Выбор стратегии бэкапа (полный, дифференциальный, инкрементальный) и типа носителей. Установка и настройка системы резервного копирования (Veeam Backup, Bacula, rsync). Создание расписания резервного копирования критически важных данных и конфигураций. Выполнение тестового восстановления данных из резервной копии с проверкой целостности. Моделирование сбоя (удаление файлов, выход из строя диска) и восстановление системы из бэкапа. Разработка документации по процедуре резервного копирования и восстановления. Оценка времени восстановления и подготовка отчёта.	
Тема 3.2. Управление инцидентами ИБ и анализ журналов событий	Содержание	12
	Изучение типов инцидентов ИБ и жизненного цикла управления инцидентами (обнаружение, анализ, локализация, ликвидация). Настройка сбора и централизованного хранения журналов событий (ELK Stack, Splunk или Graylog). Корреляция событий и создание правил оповещения для типовых атак (брутфорс, сканирование, вредоносный трафик).	

	Анализ реальных логов (предоставленных руководителем практики) и выявление признаков компрометации. Формирование записей об инцидентах в журнале учёта. Разработка процедур реагирования на инциденты (эскалация, изоляция, сбор доказательств). Составление отчёта о расследовании инцидента и плана по предотвращению повторения. Проведение учебной тренировки по реагированию на инцидент в рамках группы.	
Тема 3.3. Организация защищенного удаленного доступа (VPN)	Содержание	6
	Выбор протокола VPN (OpenVPN, WireGuard, IPsec) для организации защищённого удалённого доступа. Установка и настройка VPN-сервера на базе Linux или pfSense. Генерация сертификатов и ключей, настройка аутентификации пользователей. Настройка VPN-клиента на рабочей станции (Windows/Linux) и установка защищённого соединения. Проверка шифрования трафика (анализ пакетов в Wireshark до и после подключения). Документирование параметров VPN-сети и инструкция для пользователей.	
Тема 3.4. Анализ защищенности веб-приложений	Содержание	6
	Знакомство с типовыми уязвимостями веб-приложений (OWASP Top 10). Установка уязвимого веб-приложения (DVWA, WebGoat) в лабораторной среде. Использование инструментов для анализа защищённости: OWASP ZAP, Burp Suite Community Edition. Проведение сканирования и ручного тестирования (SQL-инъекции, XSS, CSRF). Анализ полученных результатов и классификация уязвимостей. Формулировка рекомендаций по защите веб-приложения (входная валидация, экранирование, настройки сессий).	
Тема 3.5. Разработка плана реагирования на инциденты	Содержание	6
	Анализ бизнес-процессов и критических активов организации для определения приоритетов реагирования. Разработка структуры плана реагирования на инциденты (цели, роли, каналы связи, действия по этапам). Создание шаблонов документов: уведомление об инциденте, акт расследования, отчёт о закрытии.	

	Определение перечня типовых инцидентов и соответствующих сценариев реагирования (вирус, утечка, отказ в обслуживании). Проверка плана методом «столовых учений» (tabletop exercise) с группой участников. Формирование финальной версии плана реагирования и согласование с руководителем практики.	
Тема 3.6. Аудит безопасности автоматизированной системы	Содержание	6
	Разработка программы аудита безопасности для заданной автоматизированной системы. Проведение аудита конфигураций (проверка соответствия политикам, анализаторы CIS-CAT). Анализ сетевых экранов, правил доступа, учётных записей и политик паролей. Техническая проверка с использованием средств аудита (сканеры уязвимостей, анализаторы журналов). Собеседование с администраторами и пользователями для оценки соблюдения процедур. Составление финального отчёта по аудиту с перечнем нарушений, рисков и дорожной картой исправлений.	
Промежуточная аттестация в форме зачета		144

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение производственной практики

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся (далее – Профильные организации).

База прохождения производственной практики должна быть укомплектована оборудованием, техническими средствами обучения в объеме, позволяющем выполнять определенные виды работ, связанные с будущей профессиональной деятельностью обучающихся. База практики должна обеспечивать безопасные условия труда для обучающихся.

При определении мест производственной практики (по профилю специальности) для лиц с ограниченными возможностями здоровья учитываются рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации, относительно рекомендованных условий и видов труда.

3.2. Учебно-методическое обеспечение

3.2.1. Основные печатные и/или электронные издания

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии – М.: Горячая линия – Телеком, 2023
2. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности – М.: Академия, 2024
3. Запечников С.В. Криптографические методы защиты информации – М.: Юрайт, 2023
4. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения – М.: Юрайт, 2025

3.2.2. Дополнительные источники (при необходимости)

1. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности – М.: Горячая линия – Телеком, 2018
2. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях – М.: МИФИ, 2019
3. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации – М.: Академия, 2019
4. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608

«О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199

5. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.3. Общие требования к организации производственной практики

Производственная практика проводится в профильных организациях на основе договоров, заключаемых между образовательной организацией СПО и профильными организациями.

В период прохождения производственной практики обучающиеся могут зачисляться на вакантные должности, если работа соответствует требованиям программы производственной практики.

Сроки проведения производственной практики устанавливаются образовательной организацией в соответствии с ОПОП-П по специальности *10.02.05 Обеспечение информационной безопасности автоматизированных систем*.

Производственная практика реализуется в форме практической подготовки и проводится непрерывно при условии обеспечения связи между теоретическим обучением и содержанием практики.

3.4 Кадровое обеспечение процесса производственной практики

Организацию и руководство производственной практикой осуществляют руководители практики от образовательной организации и от профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Индекс ПП	Код ПК, ОК	Основные показатели оценки результата	Формы и методы контроля и оценки
ПП 02.01	ПК 2.1	ПК 2.1.1 Выполняет установку отдельных программных, программно-аппаратных средств защиты информации ПК 2.1.2 Настраивает отдельные программные, программно-аппаратные средства защиты информации	Оценка выполнения производственного задания (аттестационные листы, дневник) и задания по практике (отчет); зачёт по практике;
	ПК 2.2	ПК 2.2.1 Обеспечивает защиту информации в автоматизированных системах отдельными программными средствами ПК 2.2.2 Обеспечивает защиту информации в автоматизированных системах отдельными программно-аппаратными средствами	Оценка выполнения производственного задания (аттестационные листы, дневник) и задания по практике (отчет); зачёт по практике;
	ПК 2.3	ПК 2.3.1 Выполняет перечень работ по тестированию функций отдельных программных средств защиты информации ПК 2.3.2 Выполняет перечень работ по тестированию функций отдельных программно-аппаратных средств защиты информации	Оценка выполнения производственного задания (аттестационные листы, дневник) и задания по практике (отчет); зачёт по практике;
	ПК 2.4	ПК 2.4.1 Обработывает и хранит информацию ограниченного доступа ПК 2.4.2 Передает информацию ограниченного доступа	Оценка выполнения производственного задания (аттестационные листы, дневник) и задания по практике (отчет); зачёт по практике;
	ПК 2.5	ПК 2.5.1 Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных средств	Оценка выполнения производственного задания (аттестационные листы, дневник) и задания по практике

		ПК 2.5.2 Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программно-аппаратных средств	(отчет); зачёт по практике;
	ОК.01	выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.02	использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.03	планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.04	эффективно взаимодействовать и работать в коллективе и команде	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.
	ОК.09	пользоваться профессиональной документацией на государственном и иностранном языках.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.