

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	3
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	12

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 информационной безопасности	Тема 1.3. Защитные механизмы в современном программном обеспечении. Технические и юридические средства защиты.	6

		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 автоматизированных системах	Тема 2.5. Установка и настройка комплексного средства на примере SecretNetStudio	6
			Тема 2.6. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности.	6

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.	
Тема 1.3. Защитные механизмы в современном программном обеспечении. Технические и юридические средства защиты.	Содержание	6
	Обзор технических механизмов защиты: антивирусные движки, HIPS, межсетевые экраны (брандмауэры). Настройка встроенных защитных механизмов	

	OC (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 инструкции по применению Foremost для расследования инцидентов.	6
	Содержание	6

Тема 1.6. Построение RAID массива	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).	
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
Тема 2.3. Составление схемы защиты	Содержание Анализ структуры и топологии защищаемой информационной системы. Определение угроз и модели нарушителя для заданного сценария.	6

	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	6
	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.	
Тема 2.5. Установка и настройка комплексного средства на примере SecretNetStudio	Содержание	6
	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.	
Тема 2.6. Установка и настройка программных средств оценки защищённости и аудита информационной безопасности.	Содержание	6
	Обзор средств оценки защищённости (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. 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	Наблюдение, оценка выполнения заданий

		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	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 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)	Интерпретация результатов наблюдений за деятельностью 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 интересные профессиональные темы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики.

