

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. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	15
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	17

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	Тема 3.1. Резервное копирование и восстановление данных	12

		обеспечении работоспособности средств ИБ		
		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 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.	6
Тема 1.3 Защитные механизмы в ПО: технические и юридические средства	Содержание 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.	6
Тема 1.4 Защита информации от несанкционированного копирования	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	6

	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	6
	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	
Тема 1.6 Построение RAID-массива	Содержание	6
	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).	
Тема 1.7 Оценка эффективности средств защиты автономной АС	Содержание	6
	Разработка критериев эффективности для средств защиты автономной АС (частота ложных срабатываний, нагрузка на систему, полнота обнаружения). 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 блокированных 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.	
	Содержание	6

Тема 2.3. Составление схемы защиты	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 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.	6
Тема 2.5. Установка и настройка комплексного средства SecretNetStudio	Содержание 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.	6
Тема 2.6. Установка и настройка средств оценки защищённости и аудита ИБ	Содержание 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.	6

	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	Содержание	6
	Выбор протокола VPN (OpenVPN, WireGuard, IPsec) для организации защищённого удалённого доступа.	

удаленного доступа (VPN)	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 и задания по практике; зачёт по практике; экзамен по модулю;
	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 и задания по практике; зачёт по практике; экзамен по модулю;
	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 и задания по практике; зачёт по практике; экзамен по модулю;
	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 и задания по практике; зачёт по практике; экзамен по модулю;
	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	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;

	ОК.01	выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;
	ОК.02	использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;
	ОК.03	планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;
	ОК.04	эффективно взаимодействовать и работать в коллективе и команде	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;
	ОК.09	пользоваться профессиональной документацией на государственном и иностранном языках.	Оценка выполнения производственного задания и задания по практике; зачёт по практике; экзамен по модулю;