ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ЭКСПО-ЛИНК»

УТВЕРЖДЕНО
приказом №5 от «18» апреля 2025г.
Директор

_____/ Поздняк О.Е.

Дополнительная профессиональная программа –
программа повышения квалификации

«ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПРИКАЗА ФСТЭК №21»
(77 часов)

г. Екатеринбург - 2025 г.

Содержание программы

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Характеристика программы:

Дополнительная профессиональная программа повышения квалификации «Выполнение требований Приказа ФСТЭК №21» (далее – программа) является учебно-методическим нормативным документом, регламентирующим содержание, организационно-методические формы и трудоемкость обучения.

Дополнительная профессиональная программа повышения квалификации «Выполнение требований Приказа ФСТЭК №21» разработана в соответствии с нормами Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» с учетом требований приказа Минобрнауки России от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н), постановлением Правительства РФ от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

Таблица 1. Связь дополнительной профессиональной программы с профессиональным стандартом

Наименование программы	Наименование выбранного профессионального стандарта (одного или нескольких), ОТФ и (или) ТФ	Уровень квалификации ОТФ и (или) ТФ
Профессия «Специалист по защите информации в автоматизированных системах»	Профессиональный стандарт: «Специалист по защите информации в автоматизированных системах» ОТФ (В) Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	6

1.2 Требование к результатам освоения программы

1.2.1. Перечень профессиональных компетенций, качественное изменение которых осуществляется в результате обучения

Таблица 2. Перечень трудовых функций, качественное изменение которых осуществляется в результате обучения:

Обобщеннная трудовая функция	Код	Наименование трудовой функции
Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	B/01.6	Диагностика систем защиты информации автоматизированных систем
	B/02.6	Администрирование систем защиты информации автоматизированных систем
	B/03.6	Управление защитой информации в автоматизированных системах
	B/04.6	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций
	B/05.6	Мониторинг защищенности информации в автоматизированных системах
	B/06.6	Аудит защищенности информации в автоматизированных системах
	B/07.6	Установка и настройка средств защиты информации в автоматизированных системах
	B/08.6	Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
	B/09.6	Анализ уязвимостей внедряемой системы защиты информации
	B/10.6	Внедрение организационных мер по защите информации в автоматизированных системах

1.3 Категория обучающихся: лица, желающие поступить на дополнительную профессиональную программу, должны иметь среднее профессиональное и (или) высшее образование либо получать среднее профессиональное и (или) высшее образование.

При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего

образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании и о квалификации[1].

1.4 Объем программы (трудоемкость): общая трудоемкость 77 академических часа.

1.5 Срок освоения программы — 8 учебных недель.

1.6 Форма обучения: заочная (с применением дистанционных образовательных технологий и электронного обучения).

1.7 Документ, выдаваемый после завершения обучения: удостоверение о повышении квалификации установленного образца.

2. ЦЕЛЬ И ЗАДАЧИ ПРОГРАММЫ

2.1. Цель программы повышения квалификации «Выполнение требований Приказа ФСТЭК №21» заключается в получении теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы с требованиями по защите информации и кибербезопасности, установленным Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.

2.2. Задачи программы:

1. Обучение основам информационной безопасности:
   - Ознакомление слушателей с основными понятиями и принципами информационной безопасности.
   - Изучение нормативно-правовой базы в области защиты информации.
2. Разработка и внедрение систем защиты информации:
   - Обучение методам и средствам защиты информации в соответствии с требованиями ФСТЭК.
   - Изучение подходов к оценке и управлению рисками в области информационной безопасности.
3. Анализ и аудит информационных систем:
   - Обучение проведению аудита информационных систем на соответствие требованиям безопасности.
   - Изучение методов анализа уязвимостей и угроз.
4. Повышение квалификации специалистов:
   - Подготовка кадров, способных эффективно реализовывать требования Приказа ФСТЭК №21 в своей организации.

[1] Часть 16 статьи 76 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

- Организация курсов повышения квалификации для действующих специалистов в области информационной безопасности.

5. Практическое применение знаний:
   - Проведение практических занятий и тренингов для отработки навыков по защите информации.
   - Разработка и реализация проектов по внедрению систем защиты информации.

6. Мониторинг и оценка эффективности:
   - Обучение методам мониторинга и оценки эффективности внедренных мер по защите информации.
   - Разработка рекомендаций по улучшению систем безопасности на основе полученных данных.

7. Создание культуры безопасности:
   - Формирование у слушателей понимания важности информационной безопасности и ответственности за ее соблюдение.
   - Привлечение внимания к вопросам кибербезопасности на уровне организации.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обобщенная трудовая функция	Наименование трудовой функции	Трудовые действия	Необходимые умения	Необходимые знания
Обеспечение защиты информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации	Диагностика систем защиты информации автоматизированных систем	Обнаружение инцидентов в процессе эксплуатации автоматизированной системы Идентификация инцидентов в процессе эксплуатации автоматизированной системы Оценка защищенности автоматизированных систем с помощью типовых программных средств Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах	Определять источники и причины возникновения инцидентов Оценивать последствия выявленных инцидентов Обнаруживать нарушения правил разграничения доступа Устранять нарушения правил разграничения доступа Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах Использовать криптографические методы и средства защиты информации в автоматизированных системах	Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Критерии оценки защищенности автоматизированной системы Технические средства контроля эффективности мер защиты информации Регламент информирования персонала автоматизированной системы о выявленных инцидентах Регламент учета выявленных инцидентов Регламент устранения последствий инцидентов Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах
	Администрирование систем защиты	Установка обновлений программного обеспечения автоматизированной	Создавать, удалять и изменять учетные записи пользователей	Принципы формирования политики информационной безопасности в

	информации автоматизированных систем	системы Выполнение установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы Управление полномочиями доступа пользователей автоматизированной системы Информирование пользователей о правилах эксплуатации автоматизированной системы с учетом требований по защите информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий с персоналом на макетах или в тестовой зоне Внесение изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	автоматизированной системы Формировать политику безопасности программных компонентов автоматизированных систем Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации Использовать криптографические методы и средства защиты информации в автоматизированных системах Регистрировать события, связанные с защитой информации в автоматизированных системах Анализировать события, связанные с защитой информации в автоматизированных системах	автоматизированных системах Программно-аппаратные средства защиты информации автоматизированных систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Методы контроля эффективности защиты информации от утечки по техническим каналам Критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем Технические средства контроля эффективности мер защиты информации Принципы организации и структура систем защиты программного обеспечения автоматизированных систем Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем Основные меры по защите информации в автоматизированных системах
	Управление защитой информации в автоматизированных системах	Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Оценивать информационные риски в автоматизированных системах Классифицировать и оценивать угрозы безопасности информации Определять подлежащие защите информационные ресурсы автоматизированных систем Применять нормативные документы по	Основные методы управления защитой информации Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Методы защиты информации от несанкционированного доступа и утечки по техническим каналам

		Оценка последствий от реализации угроз безопасности информации в автоматизированной системе Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	защите от несанкционированного доступа к информации и противодействию технической разведке Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем Конфигурировать параметры системы защиты информации автоматизированных систем Применять технические средства контроля эффективности мер защиты информации	Нормативные правовые акты в области защиты информации Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций	Обнаружение неисправностей в работе системы защиты информации автоматизированной системы Устранение неисправностей в работе системы защиты информации автоматизированной системы Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных ситуаций Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций Восстановление после сбоев и отказов программного обеспечения автоматизированных систем	Применять типовые программные средства резервирования и восстановления информации в автоматизированных системах Применять средства обеспечения отказоустойчивости автоматизированных систем Классифицировать и оценивать угрозы информационной безопасности Применять программные средства обеспечения безопасности данных Документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы	Методы и способы обеспечения отказоустойчивости автоматизированных систем Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем Основные информационные технологии, используемые в автоматизированных системах Принципы построения средств защиты информации от утечки по техническим каналам Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

	Мониторинг защищенности информации в автоматизированных системах	Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты информации при выявлении новых угроз безопасности информации Анализ недостатков в функционировании системы защиты информации автоматизированной системы Устранение недостатков в функционировании системы защиты информации автоматизированной системы	Классифицировать и оценивать угрозы информационной безопасности Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем Контролировать события безопасности и действия пользователей автоматизированных систем Применять технические средства контроля эффективности мер защиты информации Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Методы защиты информации от утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	Аудит защищенности информации в автоматизированных системах	Оценка информационных рисков безопасности информации в автоматизированной системе Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем Экспертиза состояния защищенности информации автоматизированных систем Обоснование критериев эффективности функционирования защищенных	Классифицировать и оценивать угрозы безопасности информации для объекта информатизации Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем Разрабатывать политики безопасности информации автоматизированных систем Применять инструментальные средства контроля защищенности информации в автоматизированных системах	Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Способы защиты информации от несанкционированного доступа и утечки по техническим каналам Методы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам

		автоматизированных систем		Принципы построения систем защиты информации Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации
	Установка и настройка средств защиты информации в автоматизированных системах	Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы Проведение приемочных испытаний системы защиты информации автоматизированной системы Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний	Администрировать программные средства системы защиты информации автоматизированных систем Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации Проводить анализ структурных и функциональных схем защищенной автоматизированной системы Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы	Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Содержание эксплуатационной документации автоматизированной системы Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Основные меры по защите информации в автоматизированных системах Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	Разработка организационно-распорядительных документов по защите информации в автоматизированных	Определение правил и процедур управления системой защиты информации автоматизированной системы Определение правил и процедур выявления инцидентов	Классифицировать и оценивать угрозы информационной безопасности Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации Основные угрозы безопасности информации и модели нарушителя в

	системах	Определение правил и процедур мониторинга обеспечения уровня защищенности информации автоматизированной системы Определение правил и процедур защиты информации при выводе автоматизированной системы из эксплуатации Определение правил и процедур реагирования на инциденты в автоматизированной системе	Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы Контролировать эффективность принятых мер по защите информации в автоматизированных системах	автоматизированных системах Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
	Анализ уязвимостей внедряемой системы защиты информации	Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы Проведение экспертизы состояния защищенности информации автоматизированных систем Уточнение модели угроз безопасности информации автоматизированной системы Проведение предварительных испытаний системы защиты информации автоматизированной системы Проведение анализа уязвимостей автоматизированных и информационных систем	Классифицировать и оценивать угрозы безопасности информации автоматизированной системы Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	Основные методы и средства криптографической защиты информации Способы защиты информации от несанкционированного доступа и утечки по техническим каналам Способы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Содержание эксплуатационной документации автоматизированной системы

	Внедрение организационных мер по защите информации в автоматизированных системах	Проведение проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационных мер защиты информации Проведение занятий с персоналом по работе с системой защиты информации автоматизированной системы, включая проведение практических занятий на макетах или в тестовой зоне Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации Проведение проверки готовности персонала к эксплуатации системы защиты информации автоматизированной системы Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе Подготовка документов, определяющих правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации Подготовка документов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы	Реализовывать правила разграничения доступа персонала к объектам доступа Анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Консультирование персонала автоматизированной системы по комплексу мер (правилам, процедурам, практическим приемам, руководящим принципам, методам, средствам) обеспечения защиты информации Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации Конфигурировать аттестованную информационную систему и системы защиты информации информационной системы	Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации Методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты автоматизированных систем Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации Методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации Методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем

4. СОДЕРЖАНИЕ ПРОГРАММЫ
4.1. УЧЕБНЫЙ ПЛАН

2.3. Цель обучения – получение теоретических знаний и овладении практическими умениями и навыками, обеспечивающими формирование у слушателей профессиональных компетенций, необходимых для работы с требованиями по защите информации и кибербезопасности, установленным Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.

Категория слушателей – лица, желающие поступить на дополнительную профессиональную программу, должны иметь среднее профессиональное и (или) высшее образование либо получать среднее профессиональное и (или) высшее образование.
При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации выдается одновременно с получением соответствующего документа об образовании и о квалификации[2].

Трудоемкость обучения: 77 академических часов.

Форма обучения: заочная (с применением дистанционных образовательных технологий и электронного обучения).

[2] Часть 16 статьи 76 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей)	Всего часов	В том числе:			Форма промежуточной/ итоговой аттестации
			Лекции	Домашнее задание	Итоговая и промежуточная аттестация	
1	Урок 1. Нормативная база	5	1	3	1	Проверка домашнего задания
2	Урок 2. Использование SGRC-платформы SECURITM	5	1,5	2,5	1	Проверка домашнего задания
3	Урок 3. Как оптимально определить границы ИСПДн	5	1,5	2,5	1	Проверка домашнего задания
4	Урок 4. Как оптимально определить границы ИСПДн. Практика.	5	2	2	1	Проверка домашнего задания
5	Урок 5. Как смоделировать угрозы по методике ФСТЭК	5	1,5	2,5	1	Проверка домашнего задания
6	Урок 6. Как смоделировать угрозы по методике ФСТЭК. Практика	5	2	2	1	Проверка домашнего задания
7	Урок 7. Как смоделировать угрозы по методике ФСТЭК. Практика. Часть 2	5	2	2	1	Проверка домашнего задания
8	Урок 8. Порядок создания системы защиты персональных данных. Теория и практика	5	2	2	1	Проверка домашнего задания
9	Урок 9. Как спроектировать систему безопасности. Теория и практика	5	2	2	1	Проверка домашнего задания
10	Урок 10. Практическое занятие	5	2	2	1	Проверка домашнего задания
11	Урок 11. Практическое занятие №2	5	2	2	1	Проверка домашнего задания
12	Урок 12. Выбор средств защиты для реализации конкретной меры безопасности	5	1,5	2,5	1	Проверка домашнего задания
13	Урок 13. Практическое занятие №3	5	1,5	2,5	1	Проверка домашнего задания
14	Урок 14. Практическое занятие №4	5	1,5	2,5	1	Проверка домашнего задания
15	Урок 15. Внедрение системы защиты ПДн и методы контроля процессов защиты ПДн ИБ	5	1,5	2,5	1	Проверка домашнего задания

16	Итоговая аттестация	2	-	-	2	Зачет
	Итого	**77**	**25,5**	**34,5**	**17**	

4.2 Матрица соотнесения учебных предметов, курсов, дисциплин (модулей) учебного плана программы и формируемых в них профессиональных компетенций

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей)	Всего, часов	ПК 1	ПК 2	ПК 3	ПК 4	ПК 5	ПК 6	ПК 7	ПК 8	ПК 9	ПК 10
1	Урок 1. Нормативная база	5	+		+			+			+	
2	Урок 2. Использование SGRC-платформы SECURITM	5	+	+		+	+			+		+
3	Урок 3. Как оптимально определить границы ИСПДн	5	+		+				+			+
4	Урок 4. Как оптимально определить границы ИСПДн. Практика.	5	+			+		+		+		
5	Урок 5. Как смоделировать угрозы по методике ФСТЭК	5		+		+	+		+		+	
6	Урок 6. Как смоделировать угрозы по методике ФСТЭК. Практика	5	+		+		+			+		+
7	Урок 7. Как смоделировать угрозы по методике ФСТЭК. Практика. Часть 2	5		+		+		+				+
8	Урок 8. Порядок создания системы защиты персональных данных. Теория и практика	5	+						+		+	
9	Урок 9. Как спроектировать систему безопасности. Теория и практика	5		+			+		+	+		
10	Урок 10. Практическое занятие	5	+			+		+			+	
11	Урок 11. Практическое занятие №2	5		+			+			+		+
12	Урок 12. Выбор средств защиты для реализации конкретной меры безопасности	5	+		+			+			+	
13	Урок 13. Практическое занятие №3	5		+			+			+		+
14	Урок 14. Практическое занятие №4	5	+		+				+		+	
15	Урок 15. Внедрение системы защиты ПДн и методы контроля процессов защиты ПДн ИБ	5		+			+			+		+

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный график обучения является примерным, составляется и утверждается для каждой группы.

Срок освоения программы — 8 учебных недель. Режим занятий: 2-3 раза в неделю по 4-6 акад.часа.

Начало обучения — по мере набора группы.

Трудоемкость обучения по программе составляет 77 академических часов, включая итоговый контроль

№ п.п.	Наименование учебных предметов, курсов, дисциплин (модулей)	Количество часов	Период обучения/дни
1	Урок 1. Нормативная база	5	1 неделя обучения
2	Урок 2. Использование SGRC-платформы SECURITM	5	1 неделя обучения
3	Урок 3. Как оптимально определить границы ИСПДн	5	2 неделя обучения
4	Урок 4. Как оптимально определить границы ИСПДн. Практика.	5	2 неделя обучения
5	Урок 5. Как смоделировать угрозы по методике ФСТЭК	5	3 неделя обучения
6	Урок 6. Как смоделировать угрозы по методике ФСТЭК. Практика	5	3 неделя обучения
7	Урок 7. Как смоделировать угрозы по методике ФСТЭК. Практика. Часть 2	5	4 неделя обучения
8	Урок 8. Порядок создания системы защиты персональных данных. Теория и практика	5	4 неделя обучения
9	Урок 9. Как спроектировать систему безопасности. Теория и практика	5	5 неделя обучения
10	Урок 10. Практическое занятие	5	5 неделя обучения
11	Урок 11. Практическое занятие №2	5	6 неделя обучения
12	Урок 12. Выбор средств защиты для реализации конкретной меры безопасности	5	6 неделя обучения
13	Урок 13. Практическое занятие №3	5	7 неделя обучения
14	Урок 14. Практическое занятие №4	5	7 неделя обучения
15	Урок 15. Внедрение системы защиты ПДн и методы контроля процессов защиты ПДн ИБ	5	8 неделя обучения
16	Итоговая аттестация	2	8 неделя обучения
	Итого	**77**	8 недель обучения

6. СОДЕРЖАНИЕ УЧЕБНОГО ПЛАНА

Урок 1. Нормативная база
Основные нормативные документы
Знакомство с SECURITM
Домашнее задание. Познакомиться с платформой SECURITM. Зайти в систему. В Персональной команде взять на контроль Приказ ФСТЭК 21.

Урок 2. Использование SGRC-платформы SECURITM
Контроль соответствия требованиям регуляторики
Система управления ИБ
Домашнее задание. Регистрация в платформе SECURITM и самостоятельная экспресс-проверка по требованиям Приказа ФСТЭК №21, внесение реализованных меры в SGRC-платформу SECURITM.

Урок 3. Как оптимально определить границы ИСПДн
Понятия «информационная система», «информационная система персональных данных», «сервис»
Где заканчивается зона ответственности Оператора
Что должен делать провайдер хостинга
Кто является провайдером хостинга
Как проводить и отпимизировать границы провайдера хостинга
Домашнее задание. Подготовить информацию по ИТ-инфраструктуре той ИСПДн, которую в рамках практикума будем защищать.

Урок 4. Как оптимально определить границы ИСПДн. Практика.
Формирование описания объекта защиты (ИСПДн)
«Подводные камни» и сложности при формировании объекта защиты
Домашнее задание. Подготовить информацию по ИТ-инфраструктуре той ИСПДн, которую в рамках практикума будем защищать.

Урок 5. Как смоделировать угрозы по методике ФСТЭК
В каких случаях нужно определять угрозы и для чего это нужно
Порядок определения актуальных угроз
Кто может быть опасен ИС (внутренние и внешние нарушители)
Основные «подводные камни» моделирования угроз
Структура и порядок разработки документа «Модель угроз»
Домашнее задание.
1. Самостоятельно попробовать сформировать модель угроз для 1 ИСПДн:
В шаблоне заполнить всю необходимую информацию (раздел 2,3,4,5,6 Модель угроз).
При использовании СКЗИ разработать модель нарушителя ФСБ (раздел 7 Модель угроз).
2. Определить возможные угрозы с помощью excel-файла (УБИ).

3. Оценить сценарий реализации для каждой из возможной угрозы и сформировать перечень актуальных угроз (раздел 8 Модель угроз).

Урок 6. Как смоделировать угрозы по методике ФСТЭК. Практика
Разработка модели угроз
«Подводные камни» и сложности при формировании перечня актуальных угроз
Домашнее задание.
1. Самостоятельно попробовать сформировать модель угроз для 1 ИСПДн:
В шаблоне заполнить всю необходимую информацию (раздел 2,3,4,5,6 Модель угроз).
При использовании СКЗИ разработать модель нарушителя ФСБ (раздел 7 Модель угроз).
2. Определить возможные угрозы с помощью excel-файла (УБИ).
3. Оценить сценарий реализации для каждой из возможной угрозы и сформировать перечень актуальных угроз (раздел 8 Модель угроз).

Урок 7. Как смоделировать угрозы по методике ФСТЭК. Практика. Часть 2
Разработка модели угроз
«Подводные камни» и сложности при формировании перечня актуальных угроз
Домашнее задание.
1. Самостоятельно попробовать сформировать модель угроз для 1 ИСПДн:
В шаблоне заполнить всю необходимую информацию (раздел 2,3,4,5,6 Модель угроз).
При использовании СКЗИ разработать модель нарушителя ФСБ (раздел 7 Модель угроз).
2. Определить возможные угрозы с помощью excel-файла (УБИ).
3. Оценить сценарий реализации для каждой из возможной угрозы и сформировать перечень актуальных угроз (раздел 8 Модель угроз).

Урок 8. Порядок создания системы защиты персональных данных. Теория и практика
Дорожная карта создания системы защиты персональных данных
Как верно определить уровень защищенности
Как не упустить нужное и не сделать лишнего при создании системы защиты информации
Процедура формирования набора мер безопасности
Как сформировать необходимый и достаточный набор актуальных мер защиты
Домашнее задание. Необходимо сформировать итоговый набор мер защиты для Вашей ИСПДн. Данный состав мер защиты будет основой для заполнения/ уточнения данных в в SECURITM.

Урок 9. Как спроектировать систему безопасности. Теория и практика
Причины, из-за которых стоит разрабатывать проект на систему защиты
Основные требования к проектной документации
Состав и содержание проектной и рабочей документации
Процедура проектирования системы защиты персональных данных

Этапы и стадии проектных работ
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 10. Практическое занятие
Исполнение приказа №21 в SECURITM
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 11. Практическое занятие №2
Исполнение приказа №21 в SECURITM
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 12. Выбор средств защиты для реализации конкретной меры безопасности
Алгоритм выбора как средств защиты для защиты персональных данных
Нюансы применения несертифицированных средств защиты
Альтернативы закупке средств защиты
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 13. Практическое занятие №3
Исполнение приказа №21 в SECURITM
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 14. Практическое занятие №4
Исполнение приказа №21 в SECURITM
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

Урок 15. Внедрение системы защиты ПДн и методы контроля процессов защиты ПДн ИБ
Как организовать процесс внедрения средств защиты информации и ее испытания
Аттестация, аудит, пентест, оценка эффективности и оценка соответствия: в чем разница и кто может делать
Домашнее задание. Сформировать (на выбор):
1. Техническое задание
2. Эскизный технический проект на систему защиты ИСПДн вашей компании.

7. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература:

1. Петренко В. И. Защита персональных данных в информационных системах. Практикум : учебное по собие для СПО / В. И. Петренко, И. В. Мандрица. — 2 е изд., стер. — Санкт Петербург : Лань, 2022. — 108 с.
2. Федеральный закон «О персональных данных» по состоянию на 2025 год. - Москва: Эксмо, 2025. - 32 с.;
3. Андресс Джейсон Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.

Дополнительная литература:

1. Маргарита Отдельнова Обработка и управление персональными данными/ М. Отдельнова - «Автор», 2024. - 17 с.;
2. Аверченков В.И. Защита персональных данных в организации. Монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - Москва : Флинта, 2011. - 124 с.;
3. П.Б. Филиппов Использование и защита персональных данных в социальных сетях Интернета/ П.Б. Филиппов - Входит в серию «Прикладная информатика. Научные статьи» - Синергия, 2012. - 7 с.;
4. Карисса Велиз Сила конфиденциальности: почему необходимо обладать контролем над своими персональными данными и как его установить. - ООО «Феникс», 2022. - 280 с.;
5. Максуров Алексей Анатольевич Защита оборота персональных данных в киберпространстве: монография/ А.А. Максуров. - Москва: РУСАЙНС, 2025. - 124 с.

8. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

8.1. Материально-технические условия реализации программы

Программа повышения квалификации реализовывается исключительно с применением дистанционных образовательных технологий (далее – ДОТ), электронного обучения на образовательной платформе для создания и продвижения онлайн-школ Prodamus XL.

Технические средства обучения: компьютер.

В учебном процессе используется мультимедиа и оргтехника, лекции сопровождаются слайдовыми презентациями.

Учебные занятия организуются с применением электронного обучения, дистанционных образовательных технологий в виде онлайн-курса, обеспечивающих для обучающихся независимо от их места нахождения и организации, в которой они осваивают образовательную программу, достижение и оценку результатов обучения путем организации образовательной деятельности в электронной информационно-образовательной среде, к которой предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет».

Для эффективного внедрения дистанционных образовательных технологий и использования электронных образовательных ресурсов имеется качественный доступ педагогических работников и обучающихся к информационно-телекоммуникационной сети Интернет.

Услуга подключения к сети Интернет предоставляется в режиме 24 часа в сутки 7 дней в неделю без учета объемов потребляемого трафика.

Для использования дистанционных образовательных технологий педагогическому работнику предоставляется свободный доступ к средствам информационных и коммуникационных технологий.

Рабочее место оборудовано персональным Ноутбуком Hp с необходимым программным обеспечением общего и профессионального назначения (Операционная система Microsoft Office, Браузер Яндекс).

Рабочее место педагогического работника и обучающегося оборудовано персональным компьютером и компьютерной периферией (веб-камерой, микрофоном, аудиоколонками и(или) наушниками).

8.2. Организация образовательного процесса

Форма обучения – заочная с исключительным применением электронного обучения и дистанционных образовательных технологий.

Режим занятий: учебная нагрузка устанавливается не более 40 часов в неделю и составляет не более 8 часов в день.

При реализации программы используются различные формы проведения занятий: выполнение самостоятельных и домашних заданий, обмен мнениями между преподавателями и слушателями.

Выбор методов обучения для каждого занятия определяется преподавателем в соответствии с составом и уровнем подготовленности обучающихся, степенью

сложности излагаемого материала, наличием и состоянием учебного оборудования, технических средств обучения, местом и продолжительностью проведения занятий.

Теоретические занятия проводятся с целью изучения нового учебного материала. Изложение материала необходимо вести в форме, доступной для понимания обучающихся, соблюдать единство терминологии, определений и условных обозначений, соответствующих международным договорам и нормативным правовым актам. В ходе занятий преподаватель обязан соотносить новый материал с ранее изученным, дополнять основные положения примерами из практики, соблюдать логическую последовательность изложения.

Домашние занятия проводятся с целью закрепления теоретических знаний и выработки у обучающихся основных умений и навыков работы в ситуациях, максимально имитирующих реальные производственные процессы.

Обучение ведется на русском языке.

8.3 Кадровое обеспечение образовательного процесса

Реализация дополнительной профессиональной программы повышения квалификации обеспечивается педагогическими работниками организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Для проведения занятий привлекаются специалисты, соответствующие требованиям профессионального стандарта "Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования", утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 08.09.2015 № 608н.

Образовательный процесс по образовательной программе обеспечивает преподаватели, соответствующие требованиям в сфере образования. Преподаватели должны иметь высшее профессиональное образование или среднее профессиональное образование по направлению подготовки «Образование и педагогика» или в области, соответствующей преподаваемому предмету, без предъявления требований к стажу работы либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы и повышение квалификации по направлению подготовки «Образование и педагогика».

Особые условия допуска к работе - отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации.

9. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

При реализации образовательной программы оценка результатов освоения программы проводится в рамках текущего контроля успеваемости, промежуточной и итоговой аттестации.

Текущий контроль и промежуточная аттестация успеваемости осуществляется в ходе изучения тем соответствующих модулей.

Формой промежуточной аттестации является проверка домашнего задания.

Текущий контроль успеваемости

Текущий контроль успеваемости обучающихся представляет систематическую проверку учебных достижений обучающихся, проводимую преподавателем в ходе осуществления образовательной деятельности в соответствии с образовательной программой. Проведение текущего контроля успеваемости направлено на обеспечение выстраивания образовательного процесса максимально эффективным образом для достижения результатов освоения дополнительной программы. Текущий контроль результатов подготовки осуществляется преподавателем учебной группы в ходе изучения каждой темы на каждом занятии, в целях получения информации о выполнении требуемых действий в процессе учебной деятельности; о правильности выполнения требуемых действий; о соответствии формы действия данному этапу усвоения учебного материала.

Форма текущего контроля - педагогическое наблюдение, устный опрос на занятии.

Промежуточная аттестация

Промежуточная аттестация успеваемости проводится с целью получения оперативной информации о качестве усвоения обучающимися учебного материала, управления учебным процессом и совершенствования методики проведения занятий.

Форма промежуточной аттестации – оценка работ домашних занятий.

Критерии оценивания при проведении промежуточной аттестации успеваемости: правильность ответа по содержанию занятия (учитывается количество и характер ошибок при ответе); рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели).

При проведении промежуточной аттестации применятся оценочная система оценки: «удовлетворительно»/ «неудовлетворительно».

Отметка «удовлетворительно»

Домашняя работа выполнена в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно: подобрал необходимые для выполнения предлагаемой работы источники знаний, показали необходимые для проведения самостоятельных работ теоретические знания, практические умения и навыки. Работа оформлена аккуратно, в оптимальной для

фиксации результатов форме.

Отметка «неудовлетворительно»

Выставляется в том случае, когда обучающийся оказался не подготовленным к выполнению этой работы. Полученные результаты не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Обнаружено плохое знание теоретического материала и отсутствие необходимых умений.

Итоговая аттестация

Освоение дополнительной программы завершается итоговой аттестацией обучающихся.

К итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план (индивидуальный учебный план) по программе.

Форма итоговой аттестации – зачет. Зачет проводится в форме тестирования.

При проведении итоговой аттестации используются вопросы согласно Приложения 1.

По результатам итоговой аттестации выставляются «зачтено», «не зачтено».

Критерии оценивания:

0 – 10 баллов - оценка «не зачтено»;

11 – 15 баллов - оценка «зачтено».

10. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Методика проведения занятий предусматривает теоретическую подачу материала (словесные методы) с демонстрацией таблиц и наглядных пособий (наглядные методы), а так же практическую деятельность, являющуюся необходимой для закрепления информации в виде практической работы. Практические задания выполняются индивидуально каждым обучающимся. Объяснения по выполнению практического задания даются в конце учебного занятия.

Важным является тематическое построение занятия, отражающее основные закономерности и функции деятельности педагога.

В ходе образовательного процесса в целях эффективности организации учебно-творческой деятельности обучающихся, педагогом могут быть использованы следующие приемы и методы:

- объяснительно – иллюстративный, он способствует правильной организации восприятия и первичного осмысления обучающимися новой информации с помощью рассказа, демонстрации наглядного материала и технических средств,
- репродуктивный метод, он направлен на формирование умений и навыков посредством выполнения практических упражнений, проведения беседы, повторения пройденного и т.п.,
- метод проекта, он способствует индивидуализации учебного процесса, развитию самостоятельности обучающихся, правильному планированию их учебной деятельности и исследовательской работы, продуктивному завершению работы.

Все методы и приёмы обучения находятся в тесной взаимосвязи. Взаимодействие разнообразных методов и принципов работы помогает педагогу реализовать цель – повышать квалификацию в области разработки и проведения образовательного процесса с учетом специфики когнитивных функций мозга, получать учащимся теоретические и практические навыки.

Приложение 1

Вопросы для итоговой аттестации:

1 Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа;
3. реализацию права на доступ к информации;
4. все вышеперечисленное.

2. Выберите два верных принципа обработки ПД:
1. обработка персональных данных должна осуществляться на законной и справедливой основе;
2. обработка персональных данных может не ограничиваться достижением конкретных, заранее определенных и законных целей. Допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
3. допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
4. обработке подлежат только персональные данные, которые отвечают целям их обработки.

3. Допускается ли обработка персональных данных специальных категорий, если это необходимо для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно?
1. **допускается;**
2. не допускается;
3. допускается с согласия родственников субъекта ПД;
4. допускается без согласия родственников субъекта ПД.

5. Термин «информатизация общества» обозначает:
1. целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий;
2. увеличение избыточной информации, циркулирующей в обществе; 3. увеличение роли средств массовой информации;
3. введение изучения информатики во все учебные заведения страны.
6. Компьютерные вирусы – это:
1. вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера;
2. программы, которые пишутся хакерами специально для нанесения ущерба

пользователям ПК;
3. программы, являющиеся следствием ошибок в операционной системе;
4. вирусы, сходные по природе с биологическими вирусами.

7. Что относятся к правовым методам, обеспечивающим информационную безопасность:
1. разработка аппаратных средств обеспечения правовых данных;
2. разработка и установка во всех компьютерных правовых сетях журналов учета действий;
3. разработка и конкретизация правовых нормативных актов обеспечения безопасности;
4. все выше перечисленное.

8. Основные источники угроз информационной безопасности:
1. хищение жестких дисков, подключение к сети, инсайдерство;
2. перехват данных, хищение данных, изменение архитектуры системы;
3. хищение данных, подкуп системных администраторов, нарушение регламента работы;
4. все выше перечисленное.

9. Выберите виды информационной безопасности:
1. персональная, корпоративная, государственная;
2. клиентская, серверная, сетевая;
3. локальная, глобальная, смешанная;
4. все выше перечисленное.

10. Какие угрозы безопасности информации являются преднамеренными?
1. ошибки персонала;
2. открытие электронного письма, содержащего вирус;
3. не авторизованный доступ;
4. все выше перечисленное.

11. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д. это:
1. исправление персональных данных;
2. работа с персональными данными;
3. преобразование персональных данных;
4. обработка персональных данных.

12. «Персональные данные» это:
1. **любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;** 2. фамилия, имя, отчество физического лица;
2. год, месяц, дата и место рождения, адрес физического лица;

3. адрес проживания физического лица.

13. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:
1. выход в Интернет без разрешения администратора;
2. при установке компьютерных игр;
3. в случаях установки нелицензионного ПО;
4. в любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности.

14. Какие меры информационной безопасности важны для защиты данных?
1. использование одного пароля для всех аккаунтов;
2. своевременная уборка помещений, в которых находятся сервера, хранящие данные;
3. отсутствие паролей и доступ к данным для всех людей;
4. регулярное обновление паролей, шифрование данных, обучение сотрудников правилам безопасности, аутентификации субъектов и объектов доступа, антивирусная защита.

15. Что такое информация?
1. предварительно обработанные данные, которые можно применить для принятия управленческих решений;
2. сообщения, находящиеся в памяти компьютера;
3. сообщения, находящиеся в хранилищах данных;
4. сообщения, зафиксированные на машинных носителях.;