Частное образовательное учреждение
дополнительного профессионального образования
«Учебный центр Газ-Нефть-Строй»
ЧОУ ДПО «УЦГНС»

«УТВЕРЖДЕНО»
Директором ЧОУ ДПО «УЦГНС»
Назмутдинова Г.Г.
«____» _____2025г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.
ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
СИСТЕМ И СЕТЕЙ»

г. Уфа — 2025 г.

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Настоящая программа разработана на основании следующих нормативных правовых актов:
-Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями) г.;
– Федеральный закон от 7 мая 2013 г. N 99-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" и Федерального закона "О персональных данных" (с изменениями и дополнениями).;
– Постановление правительства РФ № 211 от 21 марта 2012 г. "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
- приказ ФСТЭК России №21 от 18 февраля 2013 г. "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"

1.1. Цель реализации программы.
Целью реализации программы повышения квалификации является совершенствование и (или) получение новых компетенций, необходимых для осуществления профессиональной деятельности, повышение профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), работающих в области технической защиты информации в части организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – обучающиеся).
Обучающиеся по программе повышения квалификации готовятся к решению задач профессиональной деятельности следующих типов: проектная и эксплуатационная.

1.2. Объектами профессиональной деятельности обучающихся являются:
Сотрудникам подразделений, ответственных за сбор и хранение ПД Специалистам по защите информации Руководителям служб безопасности и защиты информации Администраторам систем безопасности, сетевым администраторам
1.3. Задачами профессиональной деятельности обучающихся являются:
а) в проектной деятельности:
определение угроз безопасности персональных данных в ИСПДн;

формирование требований к обеспечению безопасности персональных данных при их обработке в ИСПДн (формирование требований к системе защиты персональных данных);
выбор организационных и технических мер, а также реализуемых ими мероприятий по обеспечению безопасности персональных данных при их

обработке в ИСПДн (разработка системы защиты персональных данных);
внедрение организационных и технических мер, а также реализуемых ими мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн (внедрение системы защиты персональных данных);
б) в эксплуатационной деятельности:
установка, настройка, испытания и техническое обслуживание программных (программно-аппаратных) средств защиты информации;
обеспечение безопасности персональных данных в ходе эксплуатации ИСПДн;
обеспечение безопасности персональных данных при выводе из эксплуатации ИСПДн организации.

1.3. Требования к квалификации поступающего на обучение

К освоению программы повышения квалификации допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности или прошедшие профессиональную переподготовку для выполнения нового вида профессиональной деятельности в области информационной безопасности, подтвержденное документом об образовании.

1.4. Планируемые результаты обучения

Процесс освоения обучающимися программы повышения квалификации направлен на совершенствование и (или) п**олучение следующих компетенций**:
а) *общепрофессиональных:*
способность использовать нормативные правовые акты, методические документы в области обеспечения безопасности персональных данных при их обработке в ИСПДн и национальные стандарты в области защиты информации в своей профессиональной деятельности;
способность использовать достижения науки и техники, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;
б) п*рофессиональных*:
в проектной деятельности:
способность определять угрозы безопасности информации в ИСПДн;
способность формировать требования к обеспечению безопасности персональных данных при их обработке в ИСПДн (формировать требования к системе защиты персональных данных);
способность выбирать организационные и технические меры, а также реализуемые ими мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн (разрабатывать систему защиты персональных данных);
способность внедрять способы и средства для обеспечения безопасности персональных данных при их обработке в ИСПДн (внедрять систему защиты персональных данных);
в эксплуатационной деятельности:
способность обеспечивать безопасность персональных данных в ходе эксплуатации ИСПДн;
способность обеспечивать безопасность персональных данных при выводе из

эксплуатации ИСПДн;
способность устанавливать, настраивать, проводить испытания и техническое обслуживание программных (программно-аппаратных) средств защиты информации.

1.5. **В результате освоения программы повышения квалификации обучающиеся должны** получить знания, умения и навыки, обеспечивающие совершенствование соответствующих компетенций.

Освоившие программу должны:

а) знать:

нормативные правовые акты, методические документы в области обеспечения безопасности персональных данных при их обработке в ИСПДн и национальные стандарты в области защиты информации;
основные понятия в области обеспечения безопасности персональных данных при их обработке в ИСПДн;
основы построения систем защиты персональных данных в ИСПДн и обеспечения их функционирования;
требования к защите персональных данных при их обработке в ИСПДн;
требования к созданию систем защиты персональных данных и обеспечению их функционирования;
этапы создания систем защиты персональных данных при их обработке в ИСПДн;
порядок оценки угроз безопасности персональных данных и структуру модели угроз безопасности персональных данных в ИСПДн;
состав и содержание мер по обеспечению безопасности персональных данных при их обработке в ИСПДн;
требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности персональных данных при их обработке в ИСПДн;
порядок внедрения систем защиты персональных данных в ИСПДн;
порядок проведения аттестации ИСПДн на соответствие требованиям о защите информации и ввод ее в действие;
порядок обеспечения защиты персональных данных в ходе эксплуатации ИСПДн;
порядок обеспечения безопасности персональных данных при выводе из эксплуатации ИСПДн или после принятия решения об окончании обработки персональных данных;

б) **уметь:**

устанавливать требования по обеспечению безопасности персональных данных при их обработке в ИСПДн;
разрабатывать модели угроз безопасности персональных данных в ИСПДн по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей ИСПДн, возможных способов реализации угроз безопасности и последствий от их реализации, анализа банка данных угроз безопасности информации;
обосновывать организационные и технические меры, подлежащие реализации в рамках систем защиты персональных данных в ИСПДн;
осуществлять выбор средств защиты информации с учетом уровня

защищенности персональных данных в ИСПДн, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
определять параметры настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности персональных данныхи устранение уязвимостей ИСПДн;
разрабатывать документы для проведения работ по аттестации ИСПДн на соответствие требованиям о защите информации;
обеспечивать безопасность персональных данных при эксплуатации ИСПДн;
обеспечивать безопасность персональных данных при выводе из эксплуатации ИСПДн;
в) **владеть навыками:**
работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности персональных данных в ИСПДн; планирования мероприятий по обеспечению безопасности персональных данных в ИСПДн;
внедрения организационных и технических мер по обеспечению безопасности персональных данных в ИСПДн;
работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения;
анализа угроз безопасности информации в ИСПДн и последствий от их реализации;
управления (администрирования) системы защиты персональных данных в ИСПДн;
управления конфигурацией системы защиты персональных данных в ИСПДн;
реагирования на компьютерные инциденты в ходе эксплуатации ИСПДн;
обеспечения действий в нештатных ситуациях в ходе эксплуатации ИСПДн;
контроля за обеспечением безопасности персональных данных в ИСПДн.

1.6. Условия реализации программы

Организация, осуществляющая образовательную деятельность, должна иметь необходимый комплект лицензионного программного обеспечения и сертифицированные средства защиты информации.

Совершенствование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций) с целью развития профессиональных навыков обучающихся.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются на лекциях, семинарах и в ходе самостоятельной работы. Умения и навыки могут быть достигнуты проведением ряда взаимосвязанных практических занятий, компьютерного моделирования последствий принимаемых решений, деловых и ролевых игр, разбором конкретных ситуаций, тренингов и др.

Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и (или) электронными изданиями основной учебной литературы . Для обучающихся обеспечен доступ к современным

профессиональным базам данных, информационным справочным и поисковым системам по тематике информационной безопасности.

1.7. Формы аттестации и оценочные материалы

Форма итоговой аттестации обучающихся, освоивших программу повышения квалификации является тестирование. Перечень тестов, используемых для проведения итоговой аттестации, сформирован на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным модулям, представленным в рабочей программе курса повышения квалификации.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается руководителем организации, осуществляющей образовательную деятельность.

В целях обеспечения объективного определения практической и теоретической подготовленности обучающихся к выполнению профессиональных задач в состав аттестационной комиссии рекомендуется включать представителей ФСТЭК России (территориальных органов ФСТЭК России).

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

1.8 Режим занятий

Режим занятий: при очной форме обучения – 6 часов учебных занятий с преподавателем и 3 часа самостоятельной работы в день, при очно-заочной форме обучения – 4-6 часов учебных занятий с преподавателем и 2-3 часа самостоятельной работы в день.

1.9. Форма обучения: заочная (дистанционная) Обучение проходит в заочной форме с применением дистанционных образовательных технологий. Слушатели могут доступно ознакомиться с учебными материалами в любое время, благодаря чему процесс обучения становится гибким и удобным.

Предоставляется возможность задать актуальные вопросы через форму обратной связи, что обеспечивает поддержку обучающихся на протяжении всего курса.

1.10. Категория обучающихся.

Сотрудникм подразделений, ответственных за сбор и хранение ПД Специалистам по защите информации, руководители служб безопасности и защиты информации, Администраторы систем безопасности, сетевые администраторы

2. УЧЕБНЫЙ ПЛАН И СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

N п/п	Наименование учебных предметов, курсов, дисциплин (модулей) и профессиональные компетенции	Всего часов	Лекции	СРС	Форма контроля
1	**Модуль 1. Введение. Основы компьютерной безопасности, источники и носители конфиденциальной информации**	**3**	**2**	**1**	Тест
1.1	Тема 1. Понятие и принципы компьютерной безопасности	1	1	-	
1.2	Тема 2. Источники и носители конфиденциальной информации, защищаемые техническими средствами.	2	1	1	
2	**Модуль 2. Основные направления деятельности в области защиты персональных данных. Обзор нормативно-правовой базы в области защиты ПДн.**	**6**	**4**	**2**	Тест
	Тема 2.1 Основные направления деятельности в области защиты персональных данных. Общие представления о защищаемой информации.	1	1	-	
2.	Тема 2.2. Обзор нормативно-правовой базы в области защиты ПДн, Федеральный закон №152 «О персональных данных» от 27.07.2006.	1	1	-	
	Тема 2.3.Обезличивание ПДн. Общие вопросы.	1	1	-	
	Тема 2.4.Определение уровней защищенности в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	2	1	1	
	Тема 2.5.Приказ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах.	1	-	1	
3.	**Модуль 3. Построение модели угроз безопасности информации систем и сетей**	**16**	**12**	**4**	Тест
3	Тема 3.1.Вводная лекция. Определение что такое модель угроз. Цели и задачи. Какие НПА включают в себя необходимость разработки модели угроз на объекте (Приказ ФСТЭК № 21 от 18 февраля 2013 с изменениями 23 марта 2017 года, Приказ ФСТЭК № 17 от 11 февраля 2013 с изменениями 15 февраля 2017 года, Правительственное постановление № 1119 от 01.11.2012 г.,	4	3	1	

Федеральный закон № 152 ст.19 ч.2;, Приказы ФСТЭК № 239 от 25.12.2017 г. и 31 от 14.03.2014 г.). Обзор документа методики оценки угроз без-опасности информации (ФСТЭК, 2021), структура по разделам документа и приложениям, положительные и негативные аспекты			
Тема 3.2. БДУ ФСТЭК. Банк данных угроз ФСТЭК, описание автоматизированного раздела, порядок работы.	2	2	-
Тема 3. 3. Построение модели угроз. Описание ИС объекта. Определение пользователей ИС	2	1	1
Тема 3.4. Построение модели угроз. Определение потенциальных нарушителей для объекта и их возможности. Определение актуальных для каждой конкретной ИС нарушителей с указанием возможных видов воздействия и способов их реализации, а также видов негативных последствий.	4	3	1
Тема 3.5 Построение модели угроз. Моделирование действий нарушителя при реализации УБИ. Построение модели угроз. Определение актуальности угроз	2	1	1
Тема 3.6. МУ как функциональная система в динамике. Описание рабочих подходов, которые можно встроить в практическую деятельность для выявления угроз и нарушителей.	2	2	-
Модуль 4. Популярные тактики злоумышленников, технические аспекты противодействия актуальным угрозам информационной безопасности			
Тема 4.1Наиболее популярные техники у злоумышленников, наиболее опасные техники и уязвимости.			
Тема 4.2Матрица Mitre Att&ck, порядок предотвращения продвижения злоумышленника в системе, особенности проведения пентеста.			
Модуль 5. Психологический портрет нарушителя			
Тема 5.1.Выявление характерологических признаков и составление психологического портрета возможного нарушителя и лояльного сотрудника в сфере информационной безопасности.			
Модуль 6. Разработка организационно-распорядительных документов по защите персональных данных. Основы оценки рисков ИБ			

Модуль 7. Фишинг - как вид интернет-мошенничества, позволяющий получить доступ к персональным данным				
Модуль 8. Основы криптографической защиты персональных данных				
Модуль 9. Аттестация объекта информатизации (относительно персональных данных)				
Модуль 10. Особенности защиты объектов КИИ, на которых происходит обработка персональных данных				
Итоговая аттестация	**2**	**2**	**-**	Тест
Всего часов	**72**	**54**	**18**	

2.2. Календарный учебный график

Период обучения	Наименование раздела
1	2
Первый день[1)]	Модуль 1. Основы обеспечения безопасности персональных данных при их обработке в ИСПДн
Второй день	Модуль 1. Основы обеспечения безопасности персональных данных при их обработке в ИСПДн
Третий день	Модуль 1. Основы обеспечения безопасности персональных данных при их обработке в ИСПДн
Четвертый день	Модуль 2 Организация работ по обеспечению безопасности персональных данных при их обработке в ИСПДн
Пятый день	Модуль 2 Организация работ по обеспечению безопасности персональных данных при их обработке в ИСПДн
Шестой день	Модуль 2 Организация работ по обеспечению безопасности персональных данных при их обработке в ИСПДн
Седьмой день	Модуль 2 Организация работ по обеспечению безопасности персональных данных при их обработке в ИСПДн
Восьмой день	Модуль 3. Контроль (мониторинг) за обеспечением уровня защищенности персональных данных, содержащихся, в ИСПДн
Девятый день	Модуль 3. Контроль (мониторинг) за обеспечением уровня защищенности персональных данных, содержащихся, в ИСПДн **Итоговая аттестация**

[1)]Даты обучения будут определены при наборе группы на обучение