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

«Обеспечение информационной безопасности в организации»

г. Уфа — 2025 г.

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1.Цель реализации программы.

Повышение квалификации нацелено на формирование профессиональных компетенций в сфере комплексного обеспечения информационной безопасности на всех уровнях информационного пространства, освоение механизмов обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации.

1.2.Планируемые результаты обучения:

Слушатель должен знать:

- основные положения правовых и нормативно-методических документов по обеспечению информационной безопасности;
- основные способы обеспечения защиты информации;
- способы защиты от вредоносных программ;
- методы защиты сетей, программного обеспечения и информационных систем от несанкционированного доступа и использования;

Слушатель должен уметь:

-анализировать угрозы информационной безопасности для различных информационных систем;

-обосновывать выбор средств защиты информации, в том числе криптографических;

-применять средства защиты информации в операционных системах,

-обслуживать и администрировать средства защиты информации.

владеть навыками работы с конкретными программными продуктами и средствами шифрования, аутентификации, сетевой защиты, защиты от несанкционированного доступа, антивирусными программами.

1.3.Программа разработана на основании и с учетом следующих НПА:

- Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (с изменениями и дополнениями)

-Приказ Министерства труда и социальной защиты РФ от 28 ноября 2022 г. N 739н "Об утверждении профессионального стандарта "Специалист по информационной безопасности в кредитно-финансовой сфере"

- приказ Минтруда России от 14.09.2022 № 533н об утверждении Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»,
- Приказ Министерства труда и социальной защиты РФ от 14 сентября 2022 г. N 536н "Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях"
- Национальный стандарт РФ ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. N 532-ст)
- Межгосударственный стандарт ГОСТ ISO/IEC 27014-2021 "Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности" (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 2 июля 2021 г. N 613-ст)

- Национальный стандарт РФ ГОСТ Р 56939-2024 "Защита информации. Разработка безопасного программного обеспечения. Общие требования"
(утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. N 1504-ст)
Национальный стандарт РФ ГОСТ Р 59548-2022 "Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. N 2-ст)
-Национальный стандарт РФ ГОСТ Р 59547-2021 "Защита информации. Мониторинг информационной безопасности. Общие положения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 июля 2021 г. N 656-ст)
-Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2021 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст)
-Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27002-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. N 416-ст)
- и др.

1.4 Компетенции (трудовые функции) в соответствии с Профессиональным стандартом (формирование новых или совершенствование имеющихся) и/или национальной рамкой квалификаций РФ.
В соответствии с профессиональным стандартом специалиста по защите информации в автоматизированных системах можно выделить следующие трудовые функции на формирование и совершенствование которых направлена программа повышения квалификации:
B/03.6 Управление защитой информации в автоматизированных системах.
B/05.6 Мониторинг защищенности информации в автоматизированных системах.
C/04.6 Внедрение организационных мер по защите информации в автоматизированных системах.

1.5.Категория слушателей: Работники ответственные за обеспечение информационной безопасности предприятий и организаций, руководящий состав, администраторы информационной безопасности, администраторы информационных систем, менеджеры, ответственные за работу с персоналом, операторы информационных систем в которых используется электронная подпись, преподаватели общеобразовательных разделов и дисциплин по информационной безопасности.

1.6.Требования к уровню подготовки поступающего на обучение Данные курсы рассчитаны на всех заинтересованных граждан, имеющих базовое высшее образование. Необходимо владение базовыми интернет- технологиями (поиск, электронная почта, знать основы информационных технологий; иметь навыки работы на персональном компьютере в ОС MS Windows XP или выше; • иметь навыки работы в пакете MS Office 2010 или выше)

1.7.Продолжительность обучения: 72 академических часа**.**

1.8.Форма обучения: заочная (дистанционная).

1.9.Требования к материально-техническому обеспечению, необходимому для реализации дополнительной профессиональной программы повышения квалификации (требования к аудитории, компьютерному классу, программному обеспечению). Наличие у слушателей высокоскоростного подключения к Интернет (не менее 5 Мбит/с), устройств для работы с мультимедийной информацией: микрофон, веб- камера, аудиоколонки или наушники; браузера Google Chrome или Chromium релиза текущего года.

1.10. Документ об образовании: удостоверение о повышении квалификации установленного образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

N п/п	Наименование учебных предметов, курсов, дисциплин (модулей) и профессиональные компетенции	Общее количество часов	Форма контроля и результат обучения
1	**Раздел 1. Основы информационной безопасности.**	12	**З**нание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации. Знание способов зашиты от вредоносных программ. Умение выполнять анализ угроз информационной безопасности для различных информационных систем.
2	**Раздел 2. Организационно-правовые методы обеспечения защиты информации.**	20	Знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности
3	**Раздел 3. Программно-технические методы обеспечения информационной безопасност**и	32	Знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования. Знание методов защиты сетей. Умение использовать электронную подпись. Умение использовать системы шифрования различного типа. Умение использовать средства защиты от несанкционированного доступа к информационным системам
4	**Раздел 4. Управление рисками информационной безопасности**	4	Знание методов оценки рисков информационной безопасности, планирования деятельности по управлению рисками ИБ и порядка проведения аудита информационной безопасности.

5	Итоговая аттестация (Электронный курс на платформе онлайн-обучения СДО)	4
	Всего часов	**72**

2.2. Календарный учебный график

Период обучения	Наименование раздела
1	2
Первый день[1)]	Раздел 1. Основы информационной безопасности.
Второй день	Раздел 1. Основы информационной безопасности. Раздел 2. Организационно-правовые методы обеспечения защиты информации.
Третий день	Раздел 2. Организационно-правовые методы обеспечения защиты информации.
Четвертый день	Раздел 2. Организационно-правовые методы обеспечения защиты информации.
Пятый день	Раздел 3. Программно-технические методы обеспечения информационной безопасности
Шестой день	Раздел 3. Программно-технические методы обеспечения информационной безопасности
Седьмой день	Раздел 3. Программно-технические методы обеспечения информационной безопасности
Восьмой день	Раздел 3. Программно-технические методы обеспечения информационной безопасности
Девятый день	**Р**аздел 4. Управление рисками информационной безопасности. Итоговая аттестации.

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