Общество с ограниченной ответственностью
«Газпром межрегионгаз инжиниринг»
(ООО «Газпром межрегионгаз инжиниринг»)

УТВЕРЖДАЮ
Первый заместитель генерального директора
ООО «Газпром межрегионгаз инжиниринг»

_____Г.Д.Петров
«_11_»_____марта_____2020 года

Программа повышения квалификации
«Основы информационной безопасности для пользователя АРМ»

(наименование программы)

16 академических часов

САНКТ-ПЕТЕРБУРГ

2020

1. Общая характеристика программы.

1.1. Цель подготовки по программе:

Цель подготовки – качественное изменение профессиональных компетенций слушателей в области информационной безопасности и защиты информации.

1.2. Компетенции, подлежащие формированию по итогам обучения.

Программа разработана в соответствии с требованиями ФГОС ВО-бакалавриат по направлению 09.03.03 «Прикладная информатика» (Приказ Минобрнауки России от 19.09.2017 N 922, зарегистрировано в Минюсте России 12.10.2017 № 48531).

Основные профессиональные компетенции, подлежащие формированию по итогам обучения представлены в таблице.

№ компетенции	Категория слушателей	Описание компетенции/ готовность к выполнению трудовых действий в разрезе видов профессиональной деятельности
ПК.1	Лица, имеющие среднее профессиональное образование или высшее образование.	Использование существующих методов и способов защиты информации.

1.3. Требования к образованию и обучению.

Среднее профессиональное образование - программы подготовки специалистов среднего звена или высшее образование.

1.4. Трудоемкость обучения.

Нормативная трудоемкость обучения по данной программе –16 ак. часа, включая все виды аудиторной и внеаудиторной учебной работы слушателя.

1.5. Форма обучения.

С частичным отрывом от работы, с использованием дистанционных образовательных технологий.

1.6. Режим занятий.

При любой форме обучения учебная нагрузка устанавливается не более 54 ак. часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.7. Требования к результатам освоения программы.

С целью достижения указанных в таблице п.1.2 профессиональных компетенций, обучающийся в ходе освоения программы повышения квалификации слушатель должен:

Уметь:

- Проводить анализ способов нарушений информационной безопасности;
- Использовать методы и средства защиты данных.

Знать:

- Понятие информационной безопасности;
- Виды угроз информационной безопасности;
- Методы и средства борьбы с угрозами информационной безопасности;
- Понятие политики безопасности, существующие типы политик безопасности;
- Методы криптографической защиты;
- Существующие стандарты информационной безопасности.

2.Содержание программы.

2.1. Объем программы и виды учебной работы.

Вид учебной работы	Всего часов
Общий объем программы	**16**
Теоретическое обучение	14
Практическое обучение	-
Итоговая аттестация	2

2.2. Учебный план.

№ пп	Наименование тем, разделов (модулей) и учебных курсов (дисциплин)	Всего часов	В том числе			Форма и методы контроля
			Теоретическое обучение, часов	Практическое обучение, часов	из них ДОТ, часов	
1	2	3	5	6	7	9
1.	Общие сведения об информационной безопасности	2	2		2	
2.	Угрозы информационной безопасности	4	4		4	

3.	Программно-технические методы защиты	4	4		4	
4.	Криптографические методы защиты	4	4		4	
5.	Итоговая аттестация	2	2		2	Итоговый контроль
	Итого	16	16		16	

2.3. Содержание программы обучения.

Наименование тем, разделов дисциплины/ модуля	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов
Тема 1. Общие сведения об информационной безопасности.	Понятие информационной безопасности для пользователя АРМ. Необходимость защиты информационных систем и телекоммуникаций. Информационная безопасность в условиях функционирования глобальных сетей. Основные методы и средства защиты информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Управление доступом к данным. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	2
Тема 2. Угрозы информационной безопасности.	Понятие угрозы. Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени	4

	преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.	
Тема 3. Программно-технические методы защиты.	Особенности современных информационных систем. Факторы, влияющие на безопасность информационной системы. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.	4
Тема 4. Криптографические методы защиты.	Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования.	4

	Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.	
Итоговая аттестация	Итоговое тестирование.	2
Итого		16

3. Организационно-педагогические условия реализации программы

3.1. Кадровое обеспечение программы.

Кадровые условия: реализация программы обеспечивается педагогическими кадрами, имеющими, высшее профессиональное образование, соответствующее профилю дисциплины/ модуля и опыт практической деятельности в соответствующей сфере.

3.2. Оценка качества освоения программы.

Оценка качества освоения программы включает итоговую аттестацию слушателей. Итоговая аттестация реализуется в виде итогового тестирования.

3.3. Вид документов, подтверждающих повышение квалификации слушателями.

Слушателям после успешного окончания обучения и сдачи итоговой аттестации работы выдается документ установленного образца – удостоверение о повышении квалификации.

3.4. Материально-технические условия реализации программы.

Автоматизированное рабочее место (АРМ):

- Процессор: 32- или 64-разрядный процессор с тактовой частотой 1 ГГц или выше с набором инструкций SSE2;
- Операционная система: Windows 7 или более поздняя версия, Windows Server 2008 R2 или Windows Server 2012;
- Оперативная память: 1 ГБ (для 32-разрядных систем); 2 ГБ (для 64-разрядных систем);
- Свободное место на жестком диске: 3 ГБ свободного места на диске;
- Монитор: разрешение 1280 x 800;
- Графический процессор: для использования аппаратного ускорения требуется видеоадаптер, поддерживающий DirectX 10.

Подключение к Интернету.

3.5. Информационное обеспечение программы.

Учебники, учебные и справочные пособия:

1. Васильков А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2015**.** - 368 с.
2. Гришина Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с.
3. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2017. - 336 с.
4. Мельников В.П. Информационная безопасность и защита информации / В.П. Мельников. - М.: Академия, 2016**.** - 282 с.
5. Партыка Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2016**.** - 368 с.
7. Степанов Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2017**.** - 304 с.
8. Федоров А. В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. - М.: МГИМО-Университет, 2017**.** - 220 с.
9. Шаньгин В.Ф. Информационная безопасность и защита информации / Шаньгин В.Ф. - М.: ДМК Пресс, 2017. - 249 с.

3.6 Электронная версия учебно-методического комплекта программы

Содержание электронной версии учебно-методического комплекта программы:

- программа повышения квалификации, в электронном формате;
- демонстрационные презентации, отражающие структуру и содержание учебного материала, в электронном формате;
- раздаточный материал, используемый в процессе проведения учебных занятий, в электронном формате;
- методические рекомендации для слушателей по выполнению практических занятий, в электронном формате;
- методические рекомендации для слушателей по итоговой аттестации (перечень тестовых заданий, время выполнения, критерии оценивания и пр.), в электронном формате.