МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФГАОУ ВО «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

УТВЕРЖДАЮ:
Ректор
_____ М.В. Румянцев
«__» _____ 2020 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«**Обеспечение информационной безопасности организации**»

Красноярск 2020

# I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

## 1.1. Аннотация программы

Программа повышения квалификации направлена на знакомство слушателей с современной проблематикой информационной безопасности и ее аспектами, актуальными в масштабе предприятий и организаций, приобретение и углубление знаний в области методологии информационной безопасности, правового, организационного и технического обеспечения, в т.ч. особенностями защиты информации в компьютерной и сетевой среде, защиты речевой информации, защиты персональных данных, коммерческой и служебной тайны.

Реализация программы осуществляется в дистанционном формате с применением электронного обучения.

Профессиональные компетенции, которые приобретут слушатели программы «Обеспечение информационной безопасности организации», послужат востребованным стартовым потенциалом при трудоустройстве или повысят профессиональный уровень специалиста организации в рамках имеющейся квалификации в соответствии с современными требованиями, предъявляемыми к защите информации.

## 1.2. Цель программы

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.

## 1.3. 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.

## 1.4. Планируемые результаты обучения

Слушатели в результате освоения программы повышения квалификации получат:

- знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности;
- знание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации;
- знание способов зашиты от вредоносных программ;
- знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования;
- знание методов защиты сетей;
- умение использовать электронную подпись;
- умение выполнять анализ угроз информационной безопасности для различных информационных систем;
- умение использовать системы шифрования различного типа;

- умение использовать средства защиты от несанкционированного доступа к информационным системам;
- владение навыками работы с конкретными программными продуктами и средствами шифрования, аутентификации, сетевой защиты, защиты от несанкционированного доступа, антивирусными программами.

**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).

**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.

## II. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. Учебно-тематический план

| № п/п | Наименование и содержание разделов и тем программы | Всего часов | В том числе: | | Использование средств ЭО и ДОТ | Результаты обучения |
|---|---|---|---|---|---|---|
| | | | Контактная работа | Самостоятельная работа | | |
| 1 | **Раздел 1. Основы информационной безопасности.** Основные понятия в области защиты информации. Классификация угроз безопасности информации. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в информационных системах | 12 | 4 | 8 | Электронный курс на платформе онлайн-обучения СФУ, Zoom | - Знание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации.<br>- Знание способов зашиты от вредоносных программ.<br>- Умение выполнять анализ угроз информационной безопасности для различных информационных систем. |
| 2 | **Раздел 2. Организационно-правовые методы обеспечения защиты информации.** Содержание и структура законодательства в области информационной безопасности. Законодательство Российской Федерации в области обеспечения информационной безопасности. Юридическая ответственность в сфере информационной безопасности. Регуляторы в области информационной безопасности. | 20 | 4 | 16 | Электронный курс на платформе онлайн-обучения СФУ, Zoom | - Знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности |
| 3 | **Раздел 3. Программно-технические методы обеспечения информационной безопасности.** Основы криптографии. Принципы построения и применения блочных шифров с закрытым ключом. Криптография с открытым ключом. Хеш-функции. | 36 | 8 | 28 | Электронный курс на платформе онлайн-обучения СФУ, Zoom | - Знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования.<br>- Знание методов защиты сетей.<br>- Умение использовать электронную подпись. |

| № п/п | Наименование и содержание разделов и тем программы | Всего часов | В том числе: | | Использование средств ЭО и ДОТ | Результаты обучения |
|---|---|---|---|---|---|---|
| | | | Контактная работа | Самостоятельная работа | | |
| | Электронная подпись. Удостоверяющий центр. Защита сетей. Средства и методы защиты от программных закладок. Антивирусные средства защиты информации. Механизмы защиты информации от НСД. Аутентификация пользователей. Межсетевые экраны. Современные средства защиты информации (DLP и SIEM). | | | | | - Умение использовать системы шифрования различного типа.<br>- Умение использовать средства защиты от несанкционированного доступа к информационным системам |
| | Итоговая аттестация | 4 | 4 | - | Электронный курс на платформе онлайн-обучения СФУ, Zoom | |
| | **ИТОГО** | **72** | **20** | **52** | | |

### 2.2. План учебной деятельности

| Результаты обучения | Учебные действия/формы текущего контроля | Используемые ресурсы/ инструменты/технологии |
|---|---|---|
| Знание основных способов обеспечения защиты информации, в том числе криптографических методов обеспечения конфиденциальности, целостности и аутентичности информации | Знакомство с основными способами обеспечения защиты информации. Обсуждение | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |
| Знание способов зашиты от вредоносных программ | Изучение и анализ различных механизмов защиты от вредоносных программ. Разбор практических ситуаций | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование. |
| Умение выполнять анализ угроз информационной безопасности для различных информационных систем | Знакомство с угрозами информационной безопасности. Классификация угроз. Решение кейсов | Zoom, LMS Moodle. Обсуждение в форуме. Индивидуальное задание. Тестирование |
| Знание основных положений правовых и нормативно-методических документов по обеспечению информационной безопасности | Изучение нормативно-правовой базы в области информационной безопасности. Разбор конкретных ситуаций. Судебная практика | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |
| Знание методов защиты программного обеспечения и информационных систем от несанкционированного доступа и использования | Изучение теоретических вопросов. Групповое обсуждение | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |

| Результаты обучения | Учебные действия/формы текущего контроля | Используемые ресурсы/ инструменты/технологии |
|---|---|---|
| Знание методов защиты сетей | Знакомство с методами защиты сетевой инфраструктуры организации | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |
| Умение использовать электронную подпись | Изучение основных алгоритмов электронной подписи. Обсуждение областей применения электронной подписи. Получение знаний об электронном документообороте с использованием электронной подписи. Обсуждение практик работы с электронной подписью | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |
| Умение использовать системы шифрования различного типа | Знакомство с системами шифрования различного типа | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |
| Умение использовать средства защиты от несанкционированного доступа к информационным системам | Демонстрация методов защиты программного обеспечения от НСД | Zoom, LMS Moodle. Обсуждение в форуме. Тестирование |

**2.3. Виды и содержание самостоятельной работы**

Для обеспечения программы разработаны учебно-методические материалы по всем модулям и темам программы.

Слушатели обеспечены доступом к учебно-методическим материалам в электронном виде для изучения теоретического материала и обеспечения самостоятельной работы.

Сопровождение дистанционной части программы: для изучения теоретического материала, нормативных актов и организации самостоятельной работы слушателей в системе электронного обучения СФУ (http://e.sfu-kras.ru) разработан курс, включающий в себя презентации занятий, материалы для самостоятельного изучения, диагностические инструменты, иллюстрирующие видеоматериалы, ссылки на законодательные акты по теме программы.

Слушателям обеспечен доступ в систему электронного обучения (логин, пароль) предусматривающий возможность изучения и скачивания необходимых презентационных, учебно-методических и нормативных материалов, осуществления обратной связи и контактов с преподавателями программы.

Самостоятельная работа слушателей программы ориентирована на выработку навыков эффективной профессиональной теоретической, практической и учебно-исследовательской деятельности:

– обобщение с систематизация теоретического материала в соответствии с модулями программы;

– выполнении практического задания;

– прохождение онлайн тестов.

## III. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

**3.1. Учебно-методическое обеспечение, в т.ч. электронные ресурсы в корпоративной сети СФУ и сети Интернет**

1. Информационная безопасность и защита информации [Электронный ресурс]: электрон. учеб.-метод. обеспечение дисцп. [для студентов напр. подг. 09.03.02 «Информационные системы и технологии»]/Сиб. Федерал. унт; сост: М.В. Рыбков. – 2016. – Режим доступа: https://e.sfu-kras.ru/course/view.php?id=8815.

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства : [учеб. пособие для вузов] / В.Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 544 с.
3. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: [учеб. пособие для вузов] / В. Ф. Шаньгин. – М.: ФОРУМИНФРА-М, 2010. – 592 с.
4. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: [учеб. пособие для вузов] / П.Б. Хорев. – М.: Академия, 2008. – 256 с.
5. Калинина, Н.А. Методы и средства защиты информации: учеб. пособие для специальности 230105 очн. сокр. и заочн. форм обучения / Н.А. Калинина; [отв. ред. Г.А. Доррер]. – Красноярск: СибГТУ, 2009. – 196 с.
6. Информационная безопасность открытых систем: [учеб. для вузов]: [в 2 т.] / С.В. Запечников [и др.]. – Т. 2: Средства защиты в сетях. – М. : Горячая линия – Телеком, 2008. – 558 с.
7. Партыка, Т.Л. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум НИЦ ИНФРА-М, 2014. – 5-е изд., перераб. и доп. – 432 с.
8. Прохорова, О.В. Информационная безопасность и защита информации / О.В. Прохорова. – Самара: СГАСУ (Самарский государственный архитектурно строительный университет), 2014. – 114 с.

**3.2. Информационное обеспечение (информационные обучающие системы, системы вебинаров, сетевые ресурсы хостинга видео, изображений, файлов, презентаций, программное обеспечение и др.).**

Размещенные в системе электронного обучения СФУ:

1. Набор всех необходимых для обучения ресурсов и заданий в виде элементов онлайн-курса.

2. Дополнительные ссылки и материалы в формате PDF по темам курса для самостоятельного изучения.

3. Медиатека, содержащая тематические материалы, расширяющие содержание тем курса, а также краткие резюмирующие материалы, дополнительные инструкции в различных форматах (видео, скринкасты, подкасты, интерактивные справочники, текстовые пояснения), ссылки на учебно-методические материалы для программы.

## IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

**4.1. Формы аттестации, оценочные материалы, методические материалы**

Контроль результатов обучения по программе включает в себя:

- промежуточную аттестацию в рамках практических занятий – презентация проектов, результатов групповой работы, анализа конкретных ситуаций и диагностических упражнений;
- итоговую аттестацию – тестирование.

**4.2. Требования и содержание итоговой аттестации**

Основанием для аттестации является выполнение итогового online тестирования в рамках электронного обучающего курса в системе электронного обучения СФУ.

Для проведения аттестации разработан банк тестовых заданий, по всем темам образовательной программы:

- Основы информационной безопасности
  - Основные понятия в области защиты информации.
  - Классификация угроз безопасности информации.
  - Угрозы утечки информации по техническим каналам.
  - Угрозы несанкционированного доступа к информации в информационных системах.

- Организационно-правовые методы обеспечения защиты информации
  - Содержание и структура законодательства в области информационной безопасности.
  - Законодательство Российской Федерации в области обеспечения информационной безопасности.
  - Юридическая ответственность в сфере информационной безопасности.
  - Регуляторы в области информационной безопасности.
- Программно-технические методы обеспечения защиты информации:
  - Предмет и задачи криптографии.
  - Принципы построения блочных шифров с закрытым ключом.
  - Криптографические методы защиты информации.
  - Использование электронной подписи.
  - Средства и методы защиты от программных закладок.
  - Механизмы защиты информации от НСД.
  - Аутентификация пользователей.
  - Межсетевые экраны.
  - Современные средства защиты информации (DLP и SIEM).

Банк тестовых заданий составляет 200 тестовых вопросов.

Итоговый тест в электронной системе обучения СФУ включает в себя 25 вопросов по всем разделам программы.

Тестирование ограничено по времени, результаты демонстрируются слушателям непосредственно сразу после окончания итоговой аттестации.

Программу составили:

Кандидат физ.-мат. наук _____ Вайнштейн Виталий Исаакович

Кандидат технических наук _____ Вайнштейн Юлия Владимировна

Руководитель программы:

Кандидат физ.-мат. наук _____ Вайнштейн Виталий Исаакович