**Государственное автономное профессиональное образовательное учреждение Республики Саха (Якутия)**

**«Якутский колледж связи и энергетики имени П.И. Дудкина»**



**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

**ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

**Форма обучения: очная и электронная с применением дистанционных технологий**

**2020 г.**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО**

**ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

Программа дополнительного профессионального образования разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) **10.02.05 Обеспечение информационной безопасности**, утвержденной приказом Министерства образования и науки РФ от 15.05.2014 № 541, укрупнённая группа специальностей 10.00.00 Информационная безопасность.

**1.1. Цель и планируемые результаты освоения программы дополнительного профессионального образования**

1.1.1.В результате изучения программы дополнительного профессионального образования студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| **ВД 2** | **Защита информации в автоматизированных системах программными и программно-аппаратными средствами** |
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. |

* + 1. **Общие компетенции**

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |

1.1.3. В результате освоения программы дополнительного профессионального образования студент должен:

|  |  |
| --- | --- |
| **Иметь практический опыт** | * установки, настройки программных средств защиты информации в автоматизированной системе; * обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; * тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; * решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; * применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; * учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; * работы с подсистемами регистрации событий; * выявления событий и инцидентов безопасности в автоматизированной системе. |
| **уметь** | * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; * устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; * диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; * применять программные и программно-аппаратные средства для защиты информации в базах данных; * проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; * применять математический аппарат для выполнения криптографических преобразований; * использовать типовые программные криптографические средства, в том числе электронную подпись; * применять средства гарантированного уничтожения информации; * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; * осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |
| **знать** | * особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; * методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; * типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; * основные понятия криптографии и типовых криптографических методов и средств защиты информации; * особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; * типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. |

**1.2. Количество часов, отводимое на освоение программы дополнительного профессионального образования**

Всего \_\_\_ час

**2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**2.1. Структура программы дополнительного профессионального образования** ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Коды профессиональных общих компетенций | Наименования разделов программы дополнительного профессионального образования | Объем образова-тельной программы, час. | **Объем программы дополнительного профессионального образования, час.** | | | | |
| Обучение по МДК, в час. | | | Практики | Самостоя тельная работа |
| всего,  часов | в том числе | |
| лабораторных и практических занятий | курсовая работа (проект),  часов |
| ПК 2.4  ОК 1-ОК 10 | Раздел 2. Применение криптографических средств защиты информации | **237** | **140** | 56 | – | 72 | – |
|  | **Всего:** | **237** | **140** | 56 | – | 72 | – |

**2.2. Тематический план и содержание программы дополнительного профессионального образования**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов программы дополнительного профессионального образования, междисциплинарных курсов (МДК) и тем** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)** | | **Объем часов** |
| 1 | 2 | | 3 |
| Раздел 2. Применение криптографических средств защиты информации | | | **169** |
| МДК.02.02. **Криптографические средства защиты информации** | | | **144** |
| **Введение** | | **Содержание** | **2** |
| Предмет и задачи криптографии. История криптографии. Основные термины |  |
| **Раздел 1.** Математические основы защиты информации | | |  |
| **Тема 1.1.** Математические основы криптографии | | **Содержание** | **24** |
| Элементы теории множеств. Группы, кольца, поля. |  |
| Делимость чисел. Признаки делимости. Простые и составные числа. |
| Основная теорема арифметики. Наибольший общий делитель. Взаимно  простые числа. Алгоритм Евклида для нахождения НОД. |
| Отношения сравнимости. Свойства сравнений. Модулярная арифметика. |
| Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю. |
| Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. |
| Китайская теорема об остатках. |
| Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. |
| Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда. |
| Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. |
| Арифметические операции над большими числами. |
| Эллиптические кривые и их приложения в криптографии. |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений |  |
| Проверка чисел на простоту |
| Решение задач с элементами теории чисел. |
| **Раздел 2.** Классическая криптография | | |  |
| **Тема 2.1.** Методы криптографического защиты информации | | **Содержание** | **8** |
| Классификация основных методов криптографической защиты. Методы симметричного шифрования |  |
| Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр |
| Методы перестановки. Табличная перестановка, маршрутная перестановка |
| Гаммирование. Гаммирование с конечной и бесконечной гаммами |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Применение классических шифров замены |  |
| Применение классических шифров перестановки |
| Применение метода гаммирования |
| **Тема 2.2.** Криптоанализ | | **Содержание** | **6** |
| Основные методы криптоанализа. Криптографические атаки. |  |
| Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса |
| Перспективные направления криптоанализа, квантовый криптоанализ. |
| **Тематика практических занятий и лабораторных работ** | **10** |
| Криптоанализ шифра простой замены методом анализа частотности символов |  |
| Криптоанализ классических шифров методом полного перебора ключей |
| Криптоанализ шифра Вижинера |
| **Промежуточная аттестация по МДК.02.02** | | | **2** |
| **Тема 2.3.** Поточные шифры и генераторы псевдослучайных чисел | | **Содержание учебного материала** | **4** |
| Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии |  |
| Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS. |
| **Тематика практических занятий и лабораторных работ** | **2** |
| Применение методов генерации ПСЧ |  |
| **Раздел 3. Современная криптография** | | |  |
| **Тема 3.1.** Кодирование информации. Компьютеризация шифрования. | | **Содержание учебного материала** | **6** |
| Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII |  |
| Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств |
| **Тематика практических занятий и лабораторных работ** | **8** |
| Кодирование информации |  |
| Программная реализация классических шифров |
| Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге. |
| **Тема 3.2.** Симметричные системы шифрования | | **Содержание учебного материала** | **4** |
| Общие сведения. Структурная схема симметричных криптографических систем |  |
| Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4 |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Изучение программной реализации современных симметричных шифров |  |
| **Тема 3.3.** Асимметричные системы шифрования | | **Содержание учебного материала** | **4** |
| Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. |  |
| Элементы теории чисел в криптографии с открытым ключом. |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Применение различных асимметричных алгоритмов. |  |
| Изучение программной реализации асимметричного алгоритма RSA |
| **Тема 3.4.** Аутентификация данных. Электронная подпись | | **Содержание учебного материала** | **4** |
| Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи |  |
| **Тематика практических занятий и лабораторных работ** | **8** |
| Применение различных функций хеширования, анализ особенностей хешей |  |
| Применение криптографических атак на хеш-функции. |
| Изучение программно-аппаратных средств, реализующих основные функции ЭП |
| **Тема 3.5.** Алгоритмы обмена ключей и протоколы аутентификации | | **Содержание учебного материала** | **4** |
| Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация |  |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Применение протокола Диффи-Хеллмана для обмена ключами шифрования. |  |
| Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos. |
| **Тема 3.6.** Криптозащита информации в сетях передачи данных | | **Содержание учебного материала** | **4** |
| Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр |  |
| Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP. |
| **Тема 3.7.** Защита информации в электронных платежных системах | | **Содержание учебного материала** | **4** |
| Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер |  |
| Применение криптографических протоколов для обеспечения безопасности электронной коммерции. |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей |  |
| **Тема 3.8.** Компьютерная стеганография | | **Содержание учебного материала** | **4** |
| Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. |  |
| Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ |  |
| Реализация простейших стеганографических алгоритмов |
| **Тематика самостоятельной работы при изучении МДК.02.02**   1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии | | |  |
| **Промежуточная аттестация по МДК.02.02** | | | **2** |
| **Виды самостоятельной работы при изучении раздела 2**  Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)  Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. | | |  |
| **Учебная практика раздела 2**  **Виды работ:**   * Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи | | | **25** |
| **Производственная практика по ПМ.02**  **Виды работ**  – Анализ принципов построения систем информационной защиты производственных подразделений.  – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.  – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;  – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении  – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации  – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | | **100** |
| **Практика** | | | **72** |
| **Всего:** | | | **237** |

**3.  УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**3.1. Для реализации программы дополнительного профессионального образования должны быть предусмотрены следующие специальные помещения:**

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

**3.1. Для реализации программы дополнительного профессионального образования должны быть предусмотрены следующие специальные помещения:**

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

* рабочие места студентов, оборудованные персональными компьютерами;
* лабораторные учебные макеты;
* рабочее место преподавателя;
* учебно-методическое обеспечение программы;
* интерактивная доска, комплект презентаций;
* антивирусные программные комплексы;
* программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
* программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
* средства уничтожения остаточной информации в запоминающих устройствах;
* программные средства криптографической защиты информации.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование ТМЦ | Кол-во | Дата установки  /монтажа | Инвентарный № | Техническое состояние |
| 1 | Стол ученический 2100х850х750 | 9 | 20.09.2020 |  | новое |
| 2 | Стол преподавателя металлическая основа 1600х850х750 | 3 | 20.09.2020 |  | новое |
| 3 | Кресло «Престиж» кож/зам синего цвета без ручек | 19 | 20.09.2020 |  | новое |
| 4 | Кресло «Престиж» кож/зам синего цвета с рeчrами | 1 | 20.09.2020 |  | новое |
| 5 | Шкаф металлический «Архив» | 2 | 20.09.2020 |  | новое |
| 6 | Шкаф ШРМ-312 | 1 | 20.09.2020 |  | новое |
| 7 | Шкаф (стеллаж) «Бюджет», 716×333×1810 мм, 4 полки, серый | 2 | 20.09.2020 |  | новое |
| 8 | Шкаф-вешалка | 1 | 20.09.2020 |  | новое |
| 9 | **Компьютер в комплекте**  SL i7 9700 / 32Gb DDR4 / 1000Gb HDD / 480Gb SSD / RTX2060S / 2 шт монитор 24" Samsung S240300H Black (1920x1080, LED, D-sub+HDMI, 2ms. TN, 170° / 160°, 250 cd / m2. MEGA DCR) / Клавиатура Logitech MK120 клав:черный / мышь Logitech MK120 черный/серый USB | 23 | 20.09.2020 |  | новое |
| 10 | Проектор Epson EB-W05 (LCD, WXGA 1280x800, 3300Lm, 15000:1. HDMI, USB, 1x2W speaker, lamp 10000hrs, WHITE, 2.5kg) | 1 | 20.09.2020 |  | новое |
| 11 | Экран для проектора Sakura 300x300 Motoscreen 1:1 167'' фибергласс, Gray (SCPSM-300X300FG-GR) | 1 | 20.09.2020 |  | новое |
| 12 | МФУ лазерное HP LaserJet Pro MFP 1200W | 1 | 20.09.2020 |  | новое |
| 13 | DS-l252 Купольная IP-видеокамера с ИК-подсветкой до 30м | 1 | 20.09.2020 |  | новое |
| 14 | DS-l214 Компактная IP-видеокамера с ИК-подсветкой до 10м | 1 | 20.09.2020 |  | новое |
| 15 | ПАК ViPNet IDS NS100 | 1 | 20.09.2020 |  | новое |
| 16 | ПАК ViPNet Coordinator HW100 C | 2 | 20.09.2020 |  | новое |

**3.2. Информационное обеспечение обучения**

**3.2.1 Основные печатные источники:**

1. [Баричев С.Г.,](http://techbook.ru/book_list.php?str_author=%D0%91%D0%B0%D1%80%D0%B8%D1%87%D0%B5%D0%B2%20%D0%A1.%D0%93.) [Гончаров В.В.,](http://techbook.ru/book_list.php?str_author=%D0%93%D0%BE%D0%BD%D1%87%D0%B0%D1%80%D0%BE%D0%B2%20%D0%92.%D0%92.) [Серов Р.Е.](http://techbook.ru/book_list.php?str_author=%D0%A1%D0%B5%D1%80%D0%BE%D0%B2%20%D0%A0.%D0%95.) Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017. - 175 с.
2. [Душкин А.В.,](http://techbook.ru/book_list.php?str_author=%D0%94%D1%83%D1%88%D0%BA%D0%B8%D0%BD%20%D0%90.%D0%92.) [Барсуков О.М.,](http://techbook.ru/book_list.php?str_author=%D0%91%D0%B0%D1%80%D1%81%D1%83%D0%BA%D0%BE%D0%B2%20%D0%9E.%D0%9C.) [Кравцов Е.В.,](http://techbook.ru/book_list.php?str_author=%D0%9A%D1%80%D0%B0%D0%B2%D1%86%D0%BE%D0%B2%20%D0%95.%D0%92.) [Славнов К.В.](http://techbook.ru/book_list.php?str_author=%D0%A1%D0%BB%D0%B0%D0%B2%D0%BD%D0%BE%D0%B2%20%D0%9A.%D0%92.) Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016. - 248 с.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2017. – 184 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с.
5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с
6. [Иванов М.А.](http://www.iqlib.ru/search/author.visp?name=%D0%98%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2%20%D0%9C.%D0%90.), [Чугунков И.В.](http://www.iqlib.ru/search/author.visp?name=%D0%A7%D1%83%D0%B3%D1%83%D0%BD%D0%BA%D0%BE%D0%B2%20%D0%98.%D0%92.) Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: [МИФИ](http://www.iqlib.ru/publishers/publisher/2E8D62D948D8454A81119C1E552F17DE), 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
7. Ал­фё­ров А.П., Зу­бов А.Ю., Кузь­мин А.С., Че­рё­муш­кин А.В. Ос­но­вы крип­то­гра­фии (учеб­ное по­со­бие). - М.: Ге­ли­ос АРВ, 2018. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности
8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, -  336 с. – 2018
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, -  2018
10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2018. – 416 с.

**3.2.2. Дополнительные печатные источники:**

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России   
    от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России   
    от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.   
    № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.   
    Номенклатура показателей качества. Ростехрегулирование, 2005.
39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

**3.2.3. Периодические издания:**

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

**3.2.4. Электронные источники:**

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)
2. Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://www.fstec.ru)
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)
5. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)
6. Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru/)
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\[:www.ict.edu.ru](http://www.ict.edu.ru/)
10. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

|  |  |  |
| --- | --- | --- |
| Код и наименование профессиональных и общих компетенций, формируемые в рамках программы | Критерии оценки | Методы оценки |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа | тестирование,  экзамен квалификационный,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |

|  |  |  |
| --- | --- | --- |
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | * обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;   - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы  Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам  Экзамен квалификационный |
| ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения  - обоснованность самоанализа и коррекция результатов собственной работы; |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;  - обоснованность анализа работы членов команды (подчиненных) |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | -грамотность устной и письменной речи,  - ясность формулирования и изложения мыслей |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. | - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;  - знание и использование ресурсосберегающих технологий в области телекоммуникаций |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. |

Разработчик:

Никулина Н.В., преподаватель специальных дисциплин ГАПОУ РС (Я) «Колледж связи и энергетики им. П.И. Дудкина»