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

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



**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ**

**ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ**

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

**2020 г.**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ 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 техническими средствами* и соответствующие ему профессиональные компетенции:

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| **ВД 3** | **Защита информации техническими средствами** |
| ПК 3.1. | Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. |
| ПК 3.2. | Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. |
| ПК 3.3. | Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа. |
| ПК 3.4. | Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. |
| ПК 3.5. | Организовывать отдельные работы по физической защите объектов информатизации. |

* + 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, монтажа и настройки технических средств защиты информации; * технического обслуживания технических средств защиты информации; * применения основных типов технических средств защиты информации; * выявления технических каналов утечки информации; * участия в мониторинге эффективности технических средств защиты информации; * диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; * проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; * проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; * установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. |
| уметь | * применять технические средства для криптографической защиты информации конфиденциального характера; * применять технические средства для уничтожения информации и носителей информации; * применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; * применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; * применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; * применять инженерно-технические средства физической защиты объектов информатизации |
| знать | * порядок технического обслуживания технических средств защиты информации; * номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; * физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; * порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; * методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; * номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; * основные принципы действия и характеристики технических средств физической защиты; * основные способы физической защиты объектов информатизации; * номенклатуру применяемых средств физической защиты объектов информатизации. |

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

Всего \_\_\_ час

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

**2.1. Структура дополнительного профессионального образования**

**ПМ.03 Защита информации техническими 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 3.5  ОК 01–ОК10 | **Раздел 2.** Применение инженерно-технических средств физической защиты объектов информатизации | **240** | **140** | 70 | 30 | 75 | *–* |
|  | **Всего:** | **240** | **140** | 70 | 30 | 75 | *–* |

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

|  |  |  |
| --- | --- | --- |
| **Наименование разделов и тем программы дополнительного профессионального образования, междисциплинарных курсов (МДК)** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)** | **Объем часов** |
| 1 | 2 | 3 |
| **Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты** | |  |
| **Тема 2.1** Система обнаружения комплекса инженерно-технических средств физической защиты | **Содержание** | **6** |
| Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия. |  |
| **Тематика практических занятий и лабораторных работ** | **10** |
| Монтаж датчиков пожарной и охранной сигнализации |  |
| **Тема 2.2.** Система контроля и управления доступом | **Содержание** | **8** |
| Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ. |  |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя |  |
| Рассмотрение принципов устройства, работы и применения средств контроля доступа |  |
| **Тема 2.3.** Система телевизионного наблюдения | **Содержание** | **4** |
| Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения. |  |
| **Промежуточная аттестация по МДК.03.02** | | **2** |
|  | **Тематика практических занятий и лабораторных работ** | **6** |
| Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. |  |
| **Тема 2.4.** Система сбора, обработки, отображения и документирования информации | **Содержание** | **4** |
| Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации. |  |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. |  |
| **Тема 2.5** Система воздействия | **Содержание** | **2** |
| Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия. |  |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Тематика учебных занятий формируется образовательной организацией самостоятельно |  |
| **Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты** | |  |
| **Тема 3.1** Применение инженерно-технических средств физической защиты | **Содержание** | **6** |
| Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия. |  |
| **Тематика практических занятий и лабораторных работ** | **10** |
| Тематика учебных занятий формируется образовательной организацией самостоятельно |  |
| **Тема 3.2.** Эксплуатация инженерно-технических средств физической защиты | **Содержание** | **2** |
| Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты. |  |
| **Тематика практических занятий и лабораторных работ** | **12** |
| Тематика учебных занятий формируется образовательной организацией самостоятельно |  |
| **Курсовой проект (работа)** | | **30** |
| **Тематика курсового проекта (работы)**   1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. | |
| **Тематика самостоятельной работы при изучении МДК.03.02**   * Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. * Размещение периметровых средств обнаружения на местности. * Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты. | |  |
| **Промежуточная аттестация по МДК.03.02** | | **2** |
| **Виды самостоятельной работы при изучении раздела 2 программы**  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.  Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования … | |  |
| **Учебная практика по разделу 2 программы**   1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации. | | ***25*** |
| ***Практика*** | | ***75*** |
| ***Всего*** | | ***240*** |

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

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

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

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

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

1. рабочие места студентов, оборудованные персональными компьютерами;
2. лабораторные учебные макеты;
3. аппаратные средства аутентификации пользователя;
4. средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
5. средства измерения параметров физических полей;
6. стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
7. рабочее место преподавателя;
8. учебно-методическое обеспечение программы;
9. интерактивная доска, комплект презентаций.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № 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. [Зайцев А.П.,](http://www.techbook.ru/book_list.php?str_author=%D0%97%D0%B0%D0%B9%D1%86%D0%B5%D0%B2%20%D0%90.%D0%9F.) [Мещеряков Р.В.,](http://www.techbook.ru/book_list.php?str_author=%D0%9C%D0%B5%D1%89%D0%B5%D1%80%D1%8F%D0%BA%D0%BE%D0%B2%20%D0%A0.%D0%92.) [Шелупанов А.А.](http://www.techbook.ru/book_list.php?str_author=%D0%A8%D0%B5%D0%BB%D1%83%D0%BF%D0%B0%D0%BD%D0%BE%D0%B2%20%D0%90.%D0%90.) Технические средства и методы защиты информации. 7-е изд., испр. 2016.
2. [Пеньков Т.С. Основы построения технических систем охраны периметров](http://www.twirpx.com/file/1585397/). Учебное пособие. — М. 2018.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.
4. 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
5. [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), 2019.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, -  336 с. – 2016
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, -  2016
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2016. – 416 с.

**3.2.2. Дополнительные печатные источники:**

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. 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».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
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 ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
22. 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
23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
27. 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
28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
29. 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
30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.   
    Номенклатура показателей качества. Ростехрегулирование, 2005.
38. 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.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. 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.
41. 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.
42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
50. 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 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. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\[:www.ict.edu.ru](http://www.ict.edu.ru/)
9. 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 3.5 Организовывать отдельные работы по физической защите объектов информатизации | Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации | 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»