**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ   
РОСТОВСКОЙ ОБЛАСТИ**

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ"**

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

**ОП.02 Организационное и правовое обеспечение информационной**

**безопасности**

программы подготовки специалистов среднего звена

для специальности

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

(базовой подготовки)

г. Ростов-на-Дону

2025

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  Информационной безопасности  Протокол № 7 от 15 февраля 2025 года  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Копылова О.В. | **УТВЕРЖДАЮ:**  Зам. директора по УМР  И.В. Подцатова  «28 » февраля 2025 г. |

Рабочая программа частично вариативной учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», которая входит в перечень специальностей.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчик:

Асташевская А.В. – преподаватель государственного бюджетного профессионального образовательного учреждения Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Рецензент:

Масютин А.Н. - начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма».

**СОДЕРЖАНИЕ**

1. Общая характеристика рабочей программы учебной дисциплины 4

2. Структура и содержание учебной дисциплины 8

3. Условия реализации учебной дисциплины……………………………….....14

4. Контроль и оценка результатов освоения учебной дисциплины 17

**1 Общая характеристика рабочей программы учебной дисциплины**

* 1. **Место дисциплины в структуре примерной основной профессиональной образовательной программы**.

Дисциплина ОП.02 «Организационно-правовое обеспечение информационной безопасности» входит в общепрофессиональный цикл, является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей: ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и ПМ.03 «Защита информации техническими средствами».

Рабочая программа частично-вариативной учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» является частью программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» разработана на основе ФГОС СПО.

Рабочая программа предназначена для студентов дневной формы обучения.

* 1. **Цели и задачи дисциплины – требования к результатам освоения дисциплины:**

В результате изучения учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» обучающийся должен:

**Уметь:**

У.1. Осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации;

У.2. Применять нормативные правовые акты и нормативные методические документы в области защиты информации;

У.3. Контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники;

У.4. Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

У.5. Защищать свои права в соответствии с трудовым законодательством;

У.6. Разрабатывать проекты нормативных и организационно распорядительных документов, регламентирующих работу по защите информации;

У.7. Формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;

У.8. Применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;

У.9. Применять действующую законодательную базу в области обеспечения компьютерной безопасности.

**Знать:**

З.1. Основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экс-портному контролю в данной области;

З.2. Правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны;

З.3. Нормативные документы в области обеспечения защиты информации ограниченного доступа;

З.4. Организацию ремонтного обслуживания аппаратуры и средств защиты информации;

З.5. Принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

З.6. Правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);

З.7. Нормативные методические документы, регламен-тирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизиро-ванной (информационной) системе;

З.8. Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения;

3.9. Источники и классификацию угроз информацион-ной безопасности;

З.10. Основные средства и способы обеспечения инфор-мационной безопасности, принципы построения систем защиты информации;

З.11. Основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информа-ционной безопасности и нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации.

Дисциплина ОП.02 «Организационно-правовое обеспечение информационной безопасности» способствует формированию общих компетенций ОК01-ОК04,ОК06, ОК09, ОК10 и профессиональных компетенций ПК1.4, ПК2.1, ПК2.2, ПК2.3, ПК2.4, ПК3.2, ПК3.3 по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

ПК2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

ПК2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

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.

ПК3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

Вариативная часть по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» используется на увеличение объема времени на изучение тем и выполнение практический занятий в соответствии с потребностями работодателей и спецификой деятельности колледжа, что создает реальные возможности для углубления и расширения умений и знаний будущих специалистов.

Из вариативной части на освоение частично-вариативной учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» отведено **36** **часов**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование**  **темы** | **Кол-во часов** | **Дополнительные**  **умения** | **Дополнительные**  **знания** | **Формируемые компетенции** |
| Тема 4.1. Организация ремонтного обслуживания аппаратуры и средств защиты | 2 | применять нормативные правовые акты и нормативные методические документы в области защиты информации | принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; | ПК1.3  ПК1.4  ПК3.2  ОК.04  ПК2.6  ПК 2.2  ПК 2.6 |
| Тема 4.2. Применение норм трудового законодательства при решении правовых ситуаций в сфере трудовых отношений. | 2 |
| Тема 5.1 Критическая информационная инфраструктура РФ | 4 |
| Тема 6.1. Электронная подпись как инструмент обеспечения информационной безопасности | 4 |
| Тема 7.1. Компьютерная преступность как угроза информационной безопасности | 4 |
| Практическая работа №1. Работа с нормативными документами в справочно-правовых системах «Гарант», «Консультант+» | 2 |
| Практическая работа №2. Анализ положений федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". | 2 |
| Практическая работа №5. Разработка уведомления о начале обработки персональных данных в Роскомнадзор, согласия на обработку персональных данных субъекта персональных данных. | 2 |
| Практическая работа №6. Разработка политики «Требования по обеспечению информационной безопасности». | 2 |
| Практическая работа №7. Разработка политики «Обработка персональных данных в организации» | 2 |
| Практическая работа №8. Разработка политики «Обеспечение безопасности персональных данных в организации» | 2 |
| Практическая работа №13. Работа с Государственным реестром сертифицированных средств защиты информации ФСТЭК | 2 |
| Практическая работа №14. Анализ документа ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» | 2 |
| Практическая работа №15. Анализ документа «Требования по безопасности к автоматизированному рабочему месту» | 2 |
| Практическая работа №16. Разработка должностной инструкции техника по защите информации. Жизненный цикл документа. | 2 |
| **Всего** | **36** | **-** | **-** | **-** |

**Практическая подготовка при реализации учебных дисциплин путем проведения практических и лабораторных занятий:**

|  |  |  |  |
| --- | --- | --- | --- |
| Индекс и название УД, МДК, практики | Количество часов по учебному плану на практические занятия | в том числе, практическая подготовка | Наименование тем практических работ в форме практической подготовки с учетом специфики осваиваемой специальности |
| ОП.02 «Организационное и правовое обеспечение информационной без-опасности» | 32 | 26 | Практическая работа №1. Работа с нормативными документами в справочно-правовых системах «Гарант», «Консультант+»;  Практическая работа №2. Анализ положений федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";  Практическая работа №3. Анализ положений закона РФ от 21 июля 1993 г. N 5485-I "О государственной тайне";  Практическая работа №4. Классификация защищаемой законом информации по конфиденциальности;  Практическая работа №5. Разработка уведомления о начале обработки персональных данных в Роскомнадзор, согласия на обработку персональных данных субъекта персональных данных;  Практическая работа №6. Разработка политики «Требования по обеспечению информационной безопасности»;  Практическая работа №7. Разработка политики «Обработка персональных данных в организации»;  Практическая работа №8. Разработка политики «Обеспечение безопасности персональных данных в организации»;  Практическая работа №9. Подготовка документов к лицензированию;  Практическая работа №10. Подготовка документов к сертификации. Подготовка документов к аттестации объектов информатизации;  Практическая работа №12. Работа с нормативно-методическими документами в области защиты информации;  Практическая работа №15. Анализ документа «Требования по безопасности к автоматизированному рабочему месту»;  Практическая работа №16. Разработка должностной инструкции техника по защите информации. Жизненный цикл документа. |

**Структура и содержание учебной дисциплины**

* 1. **Объем дисциплины и вид учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | **Объем часов** |
| **Объем образовательной программы** | **132** |
| **Обязательная аудиторная нагрузка (всего)** | **116** |
| в том числе: |  |
| теоретическая обучение | 84 |
| практические занятия | 32 |
| **Консультации** | **4** |
| **Самостоятельная работа** | **4** |
| Вариативные часы | 36 |
| **Промежуточная аттестация по учебной дисциплине в форме экзамена** | **8** |

2.2. Тематический план и содержание учебной дисциплины «Организационное и правовое обеспечение информационной безопасности»

| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся** | **Объем часов** | **Осваиваемые элементы компетенций** |
| --- | --- | --- | --- |
| **1** | **2** | **3** | **4** |
| **Раздел 1. Правовое обеспечение информационной безопасности** | | **50** |  |
| Тема 1.1. Введение в правовое обеспечение информационной безопасности | **Содержание учебного материала** | **8** | ОК02  ОК03  ОК06  ОК09 |
| Определение основных понятий в области информации, информационных технологий и защиты информации. Информационная безопасность государства Нормативные правовые акты РФ в области информации, информационных технологий и защиты информации. Конституционные права граждан на информацию, их реализация и возможности их ограничения | 6 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №1.** Работа с нормативными документами в справочно-правовых системах «Гарант», «Консультант+» | 2 |  |
| Тема 1.2. Информация как объект правового регулирования | **Содержание учебного материала** | **6** | ОК01  ОК02  ОК03  ОК06  ОК09 |
| Информация как объект правовых отношений. Субъекты и объекты отношений в информационной сфере. | 2 |
| Виды информации по законодательству РФ. Нормы законодательства РФ, определяющие защиту информации. | 2 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №2**. Анализ положений федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации". | 2 |  |
| Тема 1.3. Правовой режим защиты государственной тайны | **Содержание учебного материала** | **14** | ОК01  ОК02  ОК03  ОК06 |
| Государственная тайна как особый вид защищаемой информации ограниченного доступа. Законодательство РФ в области защиты государственной тайны. | 2 |
| Основные понятия, используемые в Законе РФ «О государственной тайне», и их определения. | 2 |
| Степени секретности сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне. Их засекречивание и рассекречивание. | 2 |
| Документирование сведений, составляющих государственную тайну. Реквизиты носителей сведений, составляющих государственную тайну. | 2 |
| Допуск к государственной тайне и доступ к сведениям, составляющим государственную тайну. | 2 |
| Органы защиты государственной тайны в Российской Федерации. Ответственность за нарушение правового режима защиты государственной тайны. | 2 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №3.** Анализ положений закона РФ от 21 июля 1993 г. N 5485-I "О государственной тайне" | 2 |  |
| Тема 1.4. Правовые режимы защиты конфиденциальной информации | **Содержание учебного материала** | **22** | ОК02  ОК03  ОК06  ОК09  ПК2.1 |
| Законодательство РФ в области защиты конфиденциальной информации. Виды конфиденциальной информации по законодательству РФ. Отнесение сведений к конфиденциальной информации. | 4 |
| Нормативно-правовое содержание Федерального закона «О персональных данных». | 6 |
| Документирование сведений конфиденциального характера. Защита конфиденциальной информации. Ответственность за нарушение режима защиты конфиденциальной информации | 2 |
| **Практические занятия:** | **10** |  |
| **Практическая работа №4.** Классификация защищаемой законом информации по конфиденциальности | 2 |  |
| **Практическая работа №5.** Разработка уведомления о начале обработки персональных данных в Роскомнадзор, согласия на обработку персональных данных субъекта персональных данных. | 2 |  |
| **Практическая работа №6.** Разработка политики «Требования по обеспечению информационной безопасности». | 2 |  |
| **Практическая работа №7.** Разработка политики «Обработка персональных данных в организации» | 2 |  |
| **Практическая работа №8.** Разработка политики «Обеспечение безопасности персональных данных в организации» | 2 |  |
| **Раздел 2. Лицензирование и сертификация в области защиты информации** | | **30** |  |
| Тема 2.1. Лицензирование деятельности в области защиты информации | **Содержание учебного материала** | **18** | ОК01  ОК02  ОК03  ОК09  ПК.2.4  ПК3.2  ПК3.5 |
| Основные понятия в области лицензирования и их определения | 2 |
| Нормативные правовые акты, регламентирующие лицензирование деятельности в области защиты информации | 2 |
| Виды деятельности в области защиты информации, подлежащие лицензированию | 6 |
| Участники лицензионных отношений в области защиты информации | 2 |
| Получение лицензий на деятельность в области защиты информации | 4 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №9.** Подготовка документов к лицензированию | 2 |  |
| Тема 2.2. Сертификация и аттестация по требованиям безопасности информации | **Содержание учебного материала** | **12** | ОК01  ОК02  ОК03  ОК09 |
| Основные понятия в области сертификации и аттестации по требованиям безопасности и их определения | 2 |
| Системы сертификации средств защиты информации по требованиям безопасности информации | 2 |
| Сертификация средств защиты информации по требованиям безопасности информации | 2 |
| Аттестация объектов информатизации по требованиям безопасности информации | 4 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №10.** Подготовка документов к сертификации. Подготовка документов к аттестации объектов информатизации | 2 |  |
| **Раздел 3. Организационное обеспечение информационной безопасности** | | **20** |  |
| Тема 3.1. Государственная система защиты информации в Российской Федерации, ее организационная структура | **Содержание учебного материала** | **4** | ОК02  ОК03  ОК06 |
| Основные элементы организационной основы системы обеспечения информационной безопасности РФ | 2 |
| **Практические занятия:** | **2** |  |
| **Практическая работа №11.** Разработка визуальной схемы государственной системы защиты информации в РФ | 2 |  |
| Тема 3.2. Элементы государственной системы защиты информации в Российской Федерации | **Содержание учебного материала** | **16** | ОК02  ОК03  ОК06 |
| Федеральная служба безопасности Российской Федерации, ее задачи и функции в области защиты информации и информационной безопасности | 4 |
| Федеральная служба по техническому и экспортному контрою, ее задачи, полномочия и права в области защиты информации | 4 |
| **Практические занятия:** | **8** |  |
| **Практическая работа №12.** Работа с нормативно-методическими документами в области защиты информации | 2 |  |
| **Практическая работа №13.** Работа с Государственным реестром сертифицированных средств защиты информации ФСТЭК | 2 |
| **Практическая работа №14.** Анализ документа ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» | 2 |
| **Практическая работа №15.** Анализ документа «Требования по безопасности к автоматизированному рабочему месту» | 2 |
| **Раздел 4. Организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации** | | **4** |  |
| Тема 4.1. Организация ремонтного обслуживания аппаратуры и средств защиты | **Содержание учебного материала** | **2** | ОК01  ОК02  ОК03  ПК1.3  ПК1.4  ПК3.2 |
| Изъятие компьютерной техники и носителей информации. Инструкция изъятия компьютерной техники. Исследование компьютерной техники и носителей информации, оформление результатов исследования компьютерной техники. | 2 |
| Тема 4.2. Применение норм трудового законодательства при решении правовых ситуаций в сфере трудовых отношений. | **Практические занятия:** | **2** |  |
| **Практическая работа №16.** Разработка должностной инструкции техника по защите информации. Жизненный цикл документа. | 2 | ОК02  ОК03  ОК04  ОК06  ОК09 |
| **Раздел 5. Обеспечение безопасности критической информационной инфраструктуры** | | **4** |  |
| Тема 5.1. Критическая информационная инфраструктура РФ | **Содержание учебного материала** | **4** | ОК02  ОК03  ОК06  ПК2.6 |
| Понятие и состав критической информационной инфраструктуры Российской Федерации. Безопасность КИИ. Субъекты КИИ. Понятие и компетенции ФОИВ в области безопасности КИИ. Значимые объекты КИИ и их категорирование. Деятельность ГосСОПКА. Деятельность НКЦКИ. ГосСОПКА как SIEM | 4 |
| **Раздел 6. Электронная подпись как инструмент обеспечения информационной безопасности** | | **4** |  |
| Тема 6.1. Электронная подпись как инструмент обеспечения информационной безопасности | **Содержание учебного материала** | **4** |  |
| Понятие и правовая характеристика электронного документооборота. Понятие и виды электронной подписи. Доказательственное значение электронного документа. Криптографические стандарты Российской Федерации. Доказательственное значение электронного документа. | 4 | ОК02  ОК03  ОК06  ПК2.2 |
| **Раздел 7. Компьютерная преступность как угроза информационной безопасности** | | **4** |  |
| Тема 7.1. Компьютерная преступность как угроза информационной безопасности | **Содержание учебного материала** | **4** | ОК02  ОК03  ОК06  ПК2.6 |
| Понятие компьютерной преступности и взаимосвязь между компьютерной преступностью и проблемой обеспечения информационной безопасности. Место компьютерной информации в составе преступления. Характеристика компьютерных преступлений. Характеристика лиц, совершающих компьютерные преступления. Компьютерное мошенничество, компьютерное пиратство. Преступления в сфере компьютерной информации по российскому уголовному праву. | 4 |
| **Самостоятельная работа** | | **4** |  |
| **Промежуточная аттестация по учебной дисциплине в форме экзамена** | | **8** |  |
| **Всего** | | **132** |  |

# 3 условия реализации программы дисциплины

**3.1. Требования к минимальному материально-техническому обеспечению.**

Для реализации программы учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» требуется наличие учебного кабинета **нормативного правового обеспечения информационной безопасности и лаборатории информационных технологий**.

Оборудование учебного кабинета: персональный компьютер, подключение к сети Интернет, проектор, презентации уроков, стенды, плакаты, методические пособия, справочная правовая система.

Оборудование лаборатории информационных технологий: рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»; программное обеспечение сетевого оборудования; мультимедийное оборудование; программное обеспечение (справочная правовая система).

**3.2. Информационное обеспечение реализации программы обучения.**

**3.2.1 Печатные издания**

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студ. Учреждений сред. проф. образования М. : Издательский центр «Академия», 2023. – 336 с.

**3.2.2 Основные источники**

1. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 5 декабря 2016 г. № 646)
2. Федеральный закон от 27 июля 2006 г. N 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 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»
5. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»
6. Указ Президента Российской Федерации № 188 от 6 марта 1997 года «Об утверждении перечня сведений конфиденциального характера»
7. Указ Президента РФ от 30.11.1995 №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»
8. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
9. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
10. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55
11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15 февраля 2008 г.
12. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
13. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20 марта 2012 г. № 28.
14. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17
15. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119.
16. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87.
17. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9
18. Требования безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119
19. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 30 июня 2018 г. № 131
20. 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
21. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
22. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 2 марта 2001 г. № 282
23. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения
24. ГОСТ Р 58256-2018 Управление потоками информации в информационной системе. Формат классификационных меток
25. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения
26. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания
27. 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
28. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
29. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
30. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
31. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007)
32. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
34. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования
37. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения
38. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей
39. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем
40. Р 50.1.053-2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации
41. Р 50.1.056-2005 Техническая защита информации. Основные термины и определения
42. ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
43. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
44. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции (взамен ГОСТ Р ИСО/МЭК 18028-1-2008)
45. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Электронные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
46. ГОСТ 29099-91 Сети вычислительные локальные. Термины и определения

# 4 Контроль и оценка результатов освоения учебной Дисциплины

**Контроль и оценка** результатов освоения учебной дисциплины ОП.02 «Организационное и правовое обеспечение информационной безопасности» осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований, и регламентируется локальным Положением о текущем контроле и промежуточной аттестации студентов ГБПОУ РО «РКСИ».

|  |  |
| --- | --- |
| **Результаты обучения**  **(освоенные умения, усвоенные знания и практический опыт)** | **Формы и методы контроля и оценки результатов обучения** |
| В результате освоения дисциплины обучающийся должен **уметь**: | |
| * осуществлять организационное обеспечение информационной безопасности автоматизированных (информационных) систем в рамках должностных обязанностей техника по защите информации; * применять нормативные правовые акты и нормативные методические документы в области защиты информации; * контролировать соблюдение персоналом требований по защите информации при ее обработке с использованием средств вычислительной техники; * оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; * защищать свои права в соответствии с трудовым законодательством; * разрабатывать проекты нормативных и организационно распорядительных документов, регламентирующих работу по защите информации; * формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; * применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; * применять действующую законодательную базу в области обеспечения компьютерной безопасности | Контроль знаний и умений осуществляется в ходе выполнения практических работ, промежуточной аттестации.  Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы.  Экспертное заключение преподавателя |
| В результате освоения дисциплины обучающийся должен **знать**: | |
| * основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; * правовые основы организации защиты информации, содержащей сведения, составляющие государственную тайну и информации конфиденциального характера, задачи органов защиты государственной тайны; * нормативные документы в области обеспечения защиты информации ограниченного доступа; * организацию ремонтного обслуживания аппаратуры и средств защиты информации; * принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации; * правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность); * нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации, обрабатываемой в автоматизированной (информационной) системе; * законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения; * источники и классификацию угроз информационной безопасности; * основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; * основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России, ФСТЭК России в области защиты информации. | Контроль знаний и умений осуществляется в ходе выполнения практических работ, промежуточной аттестации.  Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы.  Экспертное заключение преподавателя |

Лист согласования

**Дополнения и изменения к рабочей программе на учебный год**

Дополнения и изменения к рабочей программе на \_\_\_\_\_\_\_\_\_\_ учебный год по дисциплине Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В рабочую программу дисциплины «…» внесены следующие изменения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнения и изменения в рабочей программе дисциплины «….» обсуждены на заседании ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_