**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.04 Основы информационной безопасности**

программы подготовки специалистов среднего звена

для специальности

**10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

(базовой подготовки)

г. Ростов-на-Дону

2024

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  Информационной безопасности  Протокол № 11 от 29 июня 2024 года  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Копылова О.В. | **УТВЕРЖДАЮ:**  Зам. директора по УМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «30» август 2024 г. |

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденного приказом Министерства образования и науки Российской Федерации № 1551 от 9 декабря 2016г. (ред. от 03.07.2024 №464) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем», зарегистрированного Министерством юстиции (рег. № 44944 от 26 декабря 2016 г).

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 7

3. Условия реализации учебной дисциплины……………………………….....10

4. Контроль и оценка результатов освоения учебной дисциплины………….. 12

## 1. Общая характеристика рабочей программы учебной дисциплины

**1.1 Место дисциплины в структуре примерной основной профессиональной образовательной программы**

Рабочая программа учебной дисциплины ОП.04«Основы информационной безопасности является частью программы подготовки специалистов среднего звена по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» разработана на основе ФГОС СПО. Частично вариативная дисциплина ОП.04 «Основы информационной безопасности» входит в общепрофессиональный цикл, является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей: ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты» и ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты».

Рабочая программа предназначена для студентов дневной формы обучения.

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

В результате изучения учебной дисциплины ОП.04 «Основы информационной безопасности» обучающийся должен:

**уметь:**

* классифицировать защищаемую информацию по видам тайны и степеням секретности;
* классифицировать основные угрозы безопасности информации;

**знать:**

* сущность и понятие информационной безопасности, характеристику ее составляющих;
* место информационной безопасности в системе национальной безопасности страны;
* виды, источники и носители защищаемой информации;
* источники угроз безопасности информации и меры по их предотвращению;
* факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
* жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
* современные средства и способы обеспечения информационной безопасности;
* основные методики анализа угроз и рисков информационной безопасности.

Дисциплина ОП.04 «Основы информационной безопасности» способствует формированию общих и профессиональных компетенций по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»:

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

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

ПК 2.3. 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.

Вариативная часть по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных 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 учебную дисциплину ОП.04 «Основы информационной безопасности» отведено **42часа**:

| **Наименование темы** | **Кол-во часов** | **Дополнительные умения** | **Дополнительные знания** | **Формируемые компетенции** |
| --- | --- | --- | --- | --- |
| Практическое занятие №1. Доктрина ИБ РФ | 2 | уметь описывать объект информатизации;  * знать требования и рекомендации по технической защите конфиденциальной информации; * классифицировать нарушителей; * классифицировать вирусы. | типы нарушителей;  * различные технические средства, такие как электронные уши, средства перехвата телефонной связи, средства скрытого наблюдения и поиска, средства контроля компьютеров и сетей, средства приема, записи и управления; * сущность функционирования программных закладок;  основные возможности антивирусов. | ОК 3,  ОК 6,  ОК 9, ПК.2.4 |
| Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | 2 |
| Практическое занятие №3. Классификация защищаемой информации по степеням конфиденциальности. | 2 |
| Практическое занятие №4. Виды информации ограниченного доступа | 2 |
| Практическое занятие №5. Жизненный цикл информации ограниченного доступа | 2 |
| Практическое занятие №6. Описание объекта защиты | 2 |
| Практическое занятие №7. Определение объектов защиты на типовом объекте информатизации. | 2 |
| Практическое занятие №8. Определение угроз объекта информатизации и их классификация | 2 |
| Практическое занятие №9 ФЗ 149 | 2 |
| Практическое занятие №10 ФЗ 152 | 2 |
| Практическое занятие №14. Классификация нарушителей | 2 |
| Практическое занятие №15. Разработка политики информационной безопасности организации | 2 |
| Практическое занятие №16. Анализ стандартов информационной безопасности | 2 |
| Практическое занятие №17. Классификация вредоносных программ, режим работы антивирусов | 2 |
| Самостоятельная работа | 6 |
| Экзамен | 8 |
| **Всего** | **42** | **-** | **-** | **-** |

## 2. Структура и содержание учебной дисциплины

**2.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | **Объем часов** |
| Объем образовательной программы | 78 |
| Обязательная аудиторная нагрузка (всего) | 60 |
| в том числе: |  |
| теоретическая обучение | 22 |
| практические занятия | 38 |
| Консультации | 4 |
| Самостоятельная работа | 6 |
| Промежуточная аттестация по учебной дисциплине в форме экзамена | 8 |

Практическая подготовка при реализации учебных дисциплин путем проведения практических и лабораторных занятий занимает **38 часов**.

| **Наименование темы** | **Наименование тем практических работ в форме практической подготовки с учетом специфики осваиваемой специальности** | **Кол-во часов** |
| --- | --- | --- |
| Тема 1.1. Основные понятия и задачи информационной безопасности | Практическое занятие №1. Доктрина ИБ РФ | **2** |
| Тема 1.2. Основы защиты информации | Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.  Практическое занятие №3. Классификация защищаемой информации по степеням конфиденциальности.  Практическое занятие №4. Виды информации ограниченного доступа  Практическое занятие №5. Жизненный цикл информации ограниченного доступа | **8** |
| Тема 1.3. Угрозы безопасности защищаемой информации | Практическое занятие №6. Описание объекта защиты  Практическое занятие №7. Определение объектов защиты на типовом объекте информатизации.  Практическое занятие №8. Определение угроз объекта информатизации и их классификация | **6** |
| Тема 2.1. Нормативно- правовое регулирование защиты информации | Практическое занятие №9 ФЗ 149  Практическое занятие №10 ФЗ 152  Практическое занятие №11 Специальные требования и рекомендации по защите конфиденциальной информации  Практическое занятие №12 Основные правила и документы системы сертификации РФ в области защиты информации | **12** |
| Тема 2.2. Защита информации в автоматизированных (информационных) системах | Практическое занятие №13. Выбор мер защиты информации для автоматизированного рабочего места  Практическое занятие №14. Классификация нарушителей  Практическое занятие №15. Разработка политики информационной безопасности организации  Практическое занятие №16. Анализ стандартов информационной безопасности  Практическое занятие №17. Классификация вредоносных программ, режим работы антивирусов | **10** |
| **Всего** | | **38** |

# **2.2. Тематический план и содержание учебной дисциплины**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект)**  (если предусмотрены) | **Объем часов** | **Осваиваемые элементы компетенций** |
| **1** | **2** | **3** | **4** |
| **Раздел 1 Теоретические основы информационной безопасности** | | **34** |  |
| Тема 1.1. Основные понятия и задачи информационной безопасности | **Содержание учебного материала** | **6** | ОК 3,  ОК 6,  ОК 9,  ПК.2.4 |
| Основные понятия в области защиты информации. | 2 |
| Сущность функционирования системы защиты информации. | 2 |
| **Практические работы** | **2** |
| Практическое занятие №1. Доктрина ИБ РФ | 2 |
| Тема 1.2. Основы защиты информации | **Содержание учебного материала** | **16** | ОК 3,  ОК 6,  ОК 9,  ПК.2.4 |
| Государственная тайна | 2 |
| Конфиденциальная информация | 2 |
| Цели и задачи защиты информации. | 2 |
| Политика безопасности | 2 |
| **Практические работы** | **8** |
| Практическое занятие №2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | **2** |
| Практическое занятие №3. Классификация защищаемой информации по степеням конфиденциальности. | **2** |
| Практическое занятие №4. Виды информации ограниченного доступа | **2** |
| Практическое занятие №5. Жизненный цикл информации ограниченного доступа | **2** |
| Тема 1.3. Угрозы безопасности защищаемой информации | **Содержание учебного материала** | **12** | ОК 3,  ОК 6,  ОК 9,  ПК.2.4 |
| Понятие угрозы безопасности информации. Классификация | 2 |
| Каналы и методы несанкционированного доступа к информации | 2 |
| Уязвимости. Методы оценки уязвимости информации | 2 |
| **Практические работы** | **6** |
| Практическое занятие №6.Описание объекта защиты | 2 |
| Практическое занятие №7. Определение объектов защиты на типовом объекте информатизации. | 2 |
| Практическое занятие №8. Определение угроз объекта информатизации и их классификация | 2 |
| **Раздел 2 Методология защиты информации** | | **26** |  |
| Тема 2.1. Нормативно- правовое регулирование защиты информации | **Содержание учебного материала** | **14** | ОК 3,  ОК 6,  ОК 9,  ПК.2.4 |
| Российские и международные стандарты, определяющие требования к защите информации. Законодательные акты в области защиты информации. | 2 |
| **Практические работы** | **12** |
| Практическое занятие №9 ФЗ 149 | 4 |
| Практическое занятие №10 ФЗ 152 | 4 |
| Практическое занятие №11 Специальные требования и рекомендации по защите конфиденциальной информации | 2 |
| Практическое занятие №12 Основные правила и документы системы сертификации РФ в области защиты информации | 2 |
| Тема 2.2. Защита информации в автоматизированных (информационных) системах | **Содержание учебного материала** | **12** | ОК 3,  ОК6,  ОК 9,  ПК.2.4 |
| Виды мер и основные принципы защиты информации. | 2 |
| **Практические занятия** | **10** |
| Практическое занятие №13. Выбор мер защиты информации для автоматизированного рабочего места | 2 |
| Практическое занятие №14. Классификация нарушителей | 2 |
| Практическое занятие №15. Разработка политики информационной безопасности организации | 2 |
| Практическое занятие №16. Анализ стандартов информационной безопасности | 2 |
| Практическое занятие №17. Классификация вредоносных программ, режим работы антивирусов | 2 |
| **Обязательная аудиторная нагрузка (всего)** | | **60** |  |

## 3. Условия реализации программы дисциплины

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

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности, лаборатории информационных технологий.

Оборудование учебного кабинета: персональный компьютер, проектор, презентации уроков, стенды, плакаты, методические пособия.

Оборудование лаборатории информационных технологий: посадочные места по количеству обучающихся; рабочее место преподавателя; мультимедийное оборудование.

**3.2. Информационное обеспечение реализации программы обучения**

**3.2.1. Основные источники:**

1. Внуков Андрей Анатольевич. Основы информационной безопасности: защита информации. Изд-во ЮРАЙТ-Восток 2024 – 164 стр

2. Нестеров Сергей Александрович. Основы информационной безопасности. Учебник для СПО. Издательство Лань, 2024 – 334 стр.

3. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов. Москва: Издательство Юрайт, 2024. — 107 с.

**3.2.2. Дополнительные источники:**

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2006. - 544 с.: ил. Допущено УМО ИБ.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.

4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М.: КНОРУС, 2016.

5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

6. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2017.

7. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2018.

8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – СПб.: Изд. Питер. 2017.

9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2019.

**3.2.3. Периодические издания:**

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы 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
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Федеральный портал «Российское образование www.edu.ru
5. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
6. Российский биометрический портал www.biometrics.ru
7. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
8. Сайт Научной электронной библиотеки www.elibrary.ru

### 4. Контроль и оценка результатов освоения дисциплины

**Контроль и оценка** результатов освоения учебной дисциплины ОП.04 «Основы информационной безопасности» осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий

|  |  |  |
| --- | --- | --- |
| **Результаты обучения** | **Критерии оценки** | **Формы и методы**  **контроля и оценки**  **результатов обучения** |
| 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 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе духовно-нравственных традиционных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;  ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках; | Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.  Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности  оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;  оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;  оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;  оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с *ними самостоятельно*. | устный опрос (фронтальный, индивидуальный);  - практическая проверка знаний и умений (практические работы),  - тестирование по разделам. |

**ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В**

**РАБОЧУЮ ПРОГРАММУ**

**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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_