государственное бюджетное профессиональное образовательное учреждение Самарской области «Красноармейский государственный техникум имени Героя Социалистического Труда Николая Никифоровича Пенина»

**УТВЕРЖДАЮ**
Директор ГБПОУ СО
«Красноармейский
государственный техникум
им. Н.Н Пенина»
_____/ Ладыгина Е.А./

Подписано цифровой подписью: Ладыгина Елена Анатольевна
Дата: 2025.09.25 15:45:25 +04'00'

Приказ № 42 от 08.06. 2024

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## Оп. 05 Основы цифровой безопасности

## основной образовательной программы

## 09.01.03 Оператор информационных систем и ресурсов

профиль обучения: технический

с. Красноармейское, 2024

**СОДЕРЖАНИЕ**

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 1.1. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина ОП.05 Основы цифровой безопасности входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области цифровой безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

### 1.2. Цель и планируемые результаты освоения дисциплины:

| Код ПК, ОК | Умения | Знания |
|---|---|---|
| ОК 03, ОК 06, ОК 09, ПК 1.5 | Классифицировать защищаемую информацию по видам тайны и степеням секретности;<br>Классифицировать основные угрозы безопасности информации; | сущность и понятие цифровой безопасности, характеристику ее составляющих;<br>место цифровой безопасности в системе национальной безопасности страны;<br>виды, источники и носители защищаемой информации;<br>источники угроз безопасности информации и меры по их предотвращению;<br>факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br>жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;<br>современные средства и способы обеспечения цифровой безопасности;<br>основные методики анализа угроз и рисков цифровой безопасности; |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

| Вид учебной работы | Объем в часах |
|---|---|
| **Обязательная учебная нагрузка** | 36 |
| в том числе: | |
| теоретическое обучение | 21 |
| практические занятия | 9 |
| самостоятельная работа | 6 |
| **Промежуточная аттестация в форме дифференцированного зачета** | |

**2.2. Тематический план и содержание учебной дисциплины «Основы цифровой безопасности»**

| Наименование разделов и тем | Содержание учебного материала, практические работы, семинарские занятия, самостоятельная работа обучающихся | Объем часов |
|---|---|---|
| 1 | 2 | 3 |
| **Раздел 1. Теоретические основы цифровой безопасности** | | |
| **Тема 1.1.** Основные понятия и задачи цифровой безопасности | **Содержание учебного материала** | |
| | Понятие информации и цифровой безопасности. Информация, сообщения, информационные процессы как объекты цифровой безопасности. Обзор защищаемых объектов и систем. | 2 |
| | Понятие «угроза информации». Понятие «риска цифровой безопасности». Примеры преступлений в сфере информации и информационных технологий.<br>Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности. | |
| | Самостоятельная работа | 3 |
| **Тема 1.2.** Основы защиты информации | **Содержание учебного материала** | |
| | Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. | 4 |
| | Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. | |
| | Цели и задачи защиты информации. Основные понятия в области защиты информации. | |
| | Самостоятельная работа | 3 |
| | Элементы процесса менеджмента ИБ. Модель интеграции цифровой безопасности в основную деятельность организации. Понятие Политики безопасности. | |
| | **Практические занятия** | |
| | Определение объектов защиты на типовом объекте информатизации. | 2 |
| | Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | 2 |
| **Тема 1.3.** Угрозы безопасности защищаемой информации. | **Содержание учебного материала** | |
| | Понятие угрозы безопасности информации<br>Системная классификация угроз безопасности информации.<br>Каналы и методы несанкционированного доступа к информации<br>Уязвимости. Методы оценки уязвимости информации | 3 |
| | **Практическое занятие** | |
| | Определение угроз объекта информатизации и их классификация | 6 |

| | | |
|---|---|---|
| **Раздел 2. Методология защиты информации** | | **30** |
| **Тема 2.1.** Методологические подходы к защите информации | **Содержание учебного материала** | |
| | Анализ существующих методик определения требований к защите информации. | 4 |
| | Параметры защищаемой информациии оценка факторов, влияющих на требуемый уровень защиты информации. | |
| | Виды мер и основные принципы защиты информации. | |
| **Тема 2.2.** Нормативно правовое регулирование защиты информации | **Содержание учебного материала** | |
| | Организационная структура системы защиты информации | 4 |
| | Законодательные акты в области защиты информации. | |
| | Российские и международные стандарты, определяющие требования к защите информации. | |
| | Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации | |
| | **Практическое занятие** | |
| | Работа в справочно-правовой системе с нормативными и правовыми документами по цифровой безопасности | 3 |
| **Тема 2.3.** Защита информации в автоматизированных (информационных) системах | **Содержание учебного материала** | |
| | Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. | 4 |
| | Программные и программно-аппаратные средства защиты информации | |
| | Инженерная защита и техническая охрана объектов информатизации | |
| | Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно- | |
| | **Практическое занятие** | |
| | Выбор мер защиты информации для автоматизированного рабочего места | 1 |
| | **Промежуточная аттестация учебной дисциплине** | 1 |
| | **Всего** | **36** |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

**3.1. Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:**

**Реализация программы дисциплины требует наличия учебного кабинета информатики, лаборатории информационных технологий**

### 3.2. Информационное обеспечение обучения

1. Бубнов А. А. Основы цифровой безопа сности. -М. Академия, 2021 ЭОР elib.nntc.nnov.ru: Бубнов А. А. Основы цифровой безопасности.- М. Академия, 2021
2. ЭБС www.book.ru:
3. А.В.Бабаш,Е.К.Баранова,Ю.Н.Мельников.Информационная безопасность. Лабораторный практикум (для бакалавров) — Москва: КноРус, 2022

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИН

| Результаты обучения | Критерии оценки | Формы и методы оценки |
|---|---|---|
| **Знания:**<br><br>сущность и понятие цифровой безопасности, характеристику ее составляющих;<br><br>место цифровой безопасности в системе национальной безопасности страны;<br><br>виды, источники и носители защищаемой информации;<br><br>источники угроз безопасности информации и меры по их предотвращению;<br><br>факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;<br><br>жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;<br><br>современные средства и способы обеспечения информационной<br><br>безопасности; | Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности. | Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов<br><br>практических<br><br>занятий.<br><br>Тестирование<br><br>Дифференцированный зачет |
| **Умения:**<br><br>классифицировать защищаемую информацию по видам тайны и степеням секретности;<br><br>классифицировать основные угрозы безопасности информации; | Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности | Экспертное наблюдение в процессе практических занятий<br><br>Дифференцированный зачет |