Министерство образования, науки и молодежной политики
Нижегородской области
ГБПОУ «Пильнинский агропромышленный техникум»

# РАБОЧАЯ ПРОГРАММА
# УЧЕБНОЙ ДИСЦИПЛИНЫ
# ОП.11 Информационная безопасность

Специальность: 09.02.05 Прикладная информатика (по отраслям)

р.п.Пильна
2020 г.

РАССМОТРЕНА
ПЦК дисциплин
и модулей
профессионального
цикла
Протокол № 1
от «26» августа 2020 г.
Председатель
_____М.А. Сахарова

СОГЛАСОВАНО
Методическим советом
Протокол № 1
от «27» августа 2020 г.
Председатель
_____Т.И. Бабичева

УТВЕРЖДАЮ
Зам. директора по УПР
_____/Н.А. Завражнова/
от «27» августа 2020 г.

**Организация-разработчик**: ГБПОУ «Пильнинский агропромышленный техникум» техникум»
ГБПОУ «Пильнинский агропромышленный техникум»

**Разработчик**:

Агафонова Г.Г. – преподаватель, ГБПОУ «Пильнинский агропромышленный техникум»

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.05 Прикладная информатика (по отраслям).

**СОДЕРЖАНИЕ**


| | | |
|---|---|---|
| 1. | **ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ** | 4 |
| 2. | **СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ** | 5 |
| 3. | **УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ** | 10 |
| 4. | **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ** | 10 |

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## Информационная безопасность

### 1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена по специальности 09.02.05 Прикладная информатика (по отраслям).

### 1.2. Место дисциплины в структуре образовательной программы:

Учебная дисциплина является общепрофессиональной дисциплиной и принадлежит профессиональному циклу образовательной программы.

### 1.3. Цели и задачи учебной дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен

**уметь:**

- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации.

**знать:**

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации

**Формируемые общие компетенции:**

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

**Формируемые профессиональные компетенции:**

ПК 1.1. Обрабатывать статический информационный контент.

ПК 1.2. Обрабатывать динамический информационный контент.

ПК 1.3. Осуществлять подготовку оборудования к работе.

ПК 1.4. Настраивать и работать с отраслевым оборудованием обработки информационного контента.

ПК 1.5. Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их правильную эксплуатацию.

ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.
ПК 2.2. Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом на основе готовых спецификаций и стандартов.
ПК 2.3. Проводить отладку и тестирование программного обеспечения отраслевой направленности.
ПК 2.4. Проводить адаптацию отраслевого программного обеспечения.
ПК 2.5. Разрабатывать и вести проектную и техническую документацию.
ПК 2.6. Участвовать в измерении и контроле качества продуктов.
ПК 3.1. Разрешать проблемы совместимости программного обеспечения отраслевой направленности.
ПК 3.2. Осуществлять продвижение и презентацию программного обеспечения отраслевой направленности.
ПК 3.3. Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности.
ПК 3.4. Работать с системами управления взаимоотношениями с клиентами.
ПК 4.1. Обеспечивать содержание проектных операций.
ПК 4.2. Определять сроки и стоимость проектных операций
ПК 4.3. Определять качество проектных операций.
ПК 4.4. Определять ресурсы проектных операций.
ПК 4.5. Определять риски проектных операций.

**1.4. Количество часов на освоение программы дисциплины:**
максимальной учебной нагрузки студента 135 часов, в том числе:
обязательной аудиторной учебной нагрузки студента 90 часов;
самостоятельной работы студента 45 часов.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1 Объем учебной дисциплины и виды учебной работы

| Вид учебной работы | Количество часов |
|---|---|
| **Максимальная учебная нагрузка (всего)** | 135 |
| **Обязательная аудиторная учебная нагрузка (всего)** | 90 |
| в том числе: | |
| • Практическая работа | 20 |
| **Самостоятельная работа обучающегося (всего)** | 45 |
| в том числе: | |
| • Подготовка к устному опросу, проработка материалов по лекциям, интернет-источников. | 26 |
| • подготовка рефератов, докладов, презентаций | 19 |
| **Промежуточная аттестация в форме дифференцированного зачета** | |

**2.2. Тематический план и содержание учебной дисциплины ОП.11 Информационная безопасность**

| Наименование разделов и тем | Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся | Объем часов | Уровень усвоения |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Раздел 1. БОРЬБА С УГРОЗАМИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ** | | **66** | |
| **Тема 1.1.** Актуальность проблемы обеспечения безопасности информации | **Содержание учебного материала** | 6 | |
| | 1 Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. | | 1 |
| | 2 Угрозы информационной безопасности: классификация, источники возникновения и пути реализации | | 1,2 |
| | 3 Определение требований к уровню обеспечения информационной безопасности. | | 1,2 |
| | **Самостоятельная работа обучающихся** | 10 | |
| | Подготовка к устному опросу, проработка материалов по лекциям.<br>Подготовка рефератов на тему «Угроза информационной безопасности», «Требования к уровню обеспечения информационной безопасности» | | |
| **Тема 1.2.** Виды мер информационной безопасности | **Содержание учебного материала** | 10 | |
| | 1 Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. | | 1,2 |
| | 2 Специфические приемы управления техническими средствами. | | |
| | 3 Методы защиты от копирования. Некопируемые метки. | | |
| | 4 Защита от средств отладки и дисассемблирования. Защита от трассировки по заданному прерыванию. | | |
| | 5 Защита программ в оперативной памяти | | |

| | | | | |
|---|---|---|---|---|
| | **Практическая работа** | | | |
| | Защита информации от копирования: задание некопируемых меток | | 10 | 2 |
| | Защита программ от дисассемблирования | | | 2 |
| | Защита программ в оперативной памяти. | | | 2 |
| | Защита программ в оперативной памяти. | | | 2 |
| | Приемы работы с защищенными программами. | | | 2 |
| | **Самостоятельная работа обучающихся** | | | |
| | Подготовка к устному опросу, проработка материалов по лекциям.<br>Подготовка реферата на тему: «Сотовая связь: сеть «Мегафон», сеть «БиЛайн», сеть «Сотел», сеть «ТЕЛЕ2», сеть «Кодотел», сеть МТС» | | 20 | |
| **Тема 1.3.** Основные принципы построения систем защиты информации | **Содержание учебного материала** | | 10 | |
| | 1 | Основные защитные механизмы: идентификация и аутентификация. | | 1 |
| | 2 | Разграничение доступа. | | 1,2 |
| | 3 | Контроль целостности. | | 1,2 |
| | 4 | Криптографические механизмы конфиденциальности, целостности и аутентичности информации. | | 1,2 |
| | 5 | Обнаружение и противодействие атакам. | | 1,2 |
| **Раздел 2. БОРЬБА С ВИРУСНЫМ ЗАРАЖЕНИЕМ ИНФОРМАЦИИ** | | | **50** | |
| **Тема 2.1.** Проблема вирусного заражения и структура современных вирусов | **Содержание учебного материала** | | 14 | |
| | 1 | Компьютерный вирус: понятие, пути распространения, проявление действия вируса. | | 1,2 |
| | 2 | Структура современных вирусов: модели поведения вирусов. | | 1,2 |
| | 3 | Воздействия на программно-аппаратные средства защиты информации. | | 1,2 |
| | 4 | Программы-шпионы. | | 1 |
| | 5 | Взлом парольной защиты. | | 1 |

| | | | | |
|---|---|---|---|---|
| | 6 | Защита от воздействия вирусов. | | 1,2 |
| | 7 | Пакеты антивирусных программ | | |
| | **Практическая работа** | | 10 | |
| | Перехват вывода на экран | | | 2 |
| | Перехват ввода с клавиатуры | | | 2 |
| | Перехват и обработка файловых операций | | | 2 |
| | Особенности закладок и защита от воздействия закладок | | | 2 |
| | Установка антивирусной программы | | | 2 |
| | **Самостоятельная работа обучающихся** | | 10 | |
| | Подготовка к устному опросу, проработка материалов по лекциям.<br>Подготовка доклада на тему: «Современные вирусы».<br>Подготовка презентации на тему: «Заражение вирусами» | | | |
| **Тема 2.2.** Классификация антивирусных программ | **Содержание учебного материала** | | 16 | |
| | 1 | Виды и назначение антивирусных программ | | 1 |
| | 2 | Программы-детекторы, | | 1 |
| | 3 | Программы-доктора. | | 1 |
| | 4 | Программы-ревизоры. | | 1 |
| | 5 | Программы-фильтры | | 1 |
| | 6 | Полифаги, ревизоры, блокировщики | | 1 |
| | 7 | Профилактика заражения вирусом. | | 1,2 |
| | 8 | Средства защиты от воздействия вируса | | 1,2 |
| **Раздел 3. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** | | | **19** | |
| **Тема 3.1.** Понятие протокола. | **Содержание учебного материала** | | 14 | |
| | 1 | Опыт законодательного регулирования информатизации в России и за рубежом. | | 1 |
| | 2 | Концепция правового обеспечения информационной безопасности Российской Федерации. | | 1 |

| | | | | |
|---|---|---|---|---|
| | 3 | Стандарты и нормативно-методические документа в области обеспечения информационной безопасности. | | 1 |
| | 4 | Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации. | | 1 |
| | 5 | Состав и назначение должностных инструкций. | | 1,2 |
| | 6 | Порядок создания, утверждения и исполнения должностных инструкций | | 1 |
| | 7 | Тестирование. Дифференцированный зачет. | | 3 |
| | **Самостоятельная работа обучающихся** | | 5 | |
| | Подготовка к устному опросу, проработка материалов по лекциям.<br>Подготовка реферата на тему «Государственная система обеспечения информационной безопасности» | | | |
| **Всего:** | | | **135** | |

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

## 3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

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

Реализация программы учебной дисциплины требует наличия учебного кабинета архитектуры электронно-вычислительных систем и вычислительных систем, лаборатории обработки информации отраслевой направленности, библиотеки, читального зала с выходом в сеть Интернет.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- автоматизированное рабочее место преподавателя;

Технические средства обучения:

- компьютер с лицензионным программным обеспечением;
- мультимедийное оборудование.

Оборудование лаборатории и рабочих мест:

- автоматизированные рабочие места обучающихся;
- автоматизированное рабочее место преподавателя;
- специализированная мебель;
- комплект нормативных документов;
- рекомендации по подготовке к практическим занятиям;
- задания для проведения практических занятий;
- программное обеспечение общего и профессионального назначения.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением;
- мультимедийное оборудование.

### 3.2. Информационное обеспечение обучения

**Основные источники:**

1.Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М,2020. — 416 с. — (Среднее профессиональное образование).ISBN 978-5-16-101207-9 (ИНФРА-М, online)

**Дополнительные источники:**

1. Исаченко О.В. Программное обеспечение компьютерных сетей : учебное пособие /О.В. Исаченко. — 2-е изд., испр. и доп. — Москва : ИНФРА-М, 2020. —158 с. — (Среднее профессиональное образование).ISBN 978-5-16-108134-1 (online)
2. http://all-ib.ru/ Информационная безопасность
3. http://www.securrity.ru/ Информационная безопасность
4. http://sec-it.ru/ Всё о защите информации
5. http://www.right777.ru/protec.html электронная библиотека книг
6. http://www.proklondike.com/books/defence.html электронная библиотека книг
7. http://bookwebmaster.narod.ru/websecurity.html электронная библиотека книг

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических работ, тестирования, а также выполнения обучающимися домашних заданий, защиты доклада, самостоятельной работы.

| **Результаты обучения (освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
|---|---|
| **умения:** | |
| • применять правовые, организационные, технические и программные средства защиты информации; | Экспертная оценка выполнения и защиты практической работы, экзамен |

| | |
|---|---|
| • создавать программные средства защиты информации. | Экспертная оценка выполнения и защиты практической работы, выполнение домашних заданий, экзамен |
| **знания:** | |
| • источников возникновения информационных угроз; | Тестирование, устный опрос, оценка защиты доклада, экспертное наблюдение при выполнении практической работы , экзамен . |
| • модели и принципов защиты информации от несанкционированного доступа; | Тестирование, устный опрос, экспертное наблюдение при выполнении практической работы, экзамен |
| • методов антивирусной защиты информации; | Тестирование, устный опрос, экспертное наблюдение при выполнении практической работы, экзамен |
| • состава и методов организационно-правовой защиты информации | Тестирование, устный опрос, экспертное наблюдение при выполнении практической работы, оценка защиты доклада, экзамен |