Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский экономический университет им. Г.В. Плеханова»
**МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ**

# РАБОЧАЯ ПРОГРАММА

учебной дисциплины: ОП.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

код, специальность 09.02.05 Прикладная информатика (по отраслям)

квалификация: техник-программист

форма обучения: очная

Москва
2017

**СОГЛАСОВАНА:**
Предметной (цикловой) комиссией
**Профессиональных модулей 09.02.05**

**Протокол № 1**
**от «31» 08 2014 года**

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
**09.02.05 Прикладная информатика (по отраслям)**

**Председатель предметной (цикловой) комиссии**

Л.А. Соколова
Подпись Инициалы Фамилия

**Заместитель директора по учебной работе**

Д.А. Клопов
Подпись Инициалы Фамилия

**УТВЕРЖДЕНА:**

Директором техникума А.В. Чурилов
Подпись

**Составители (авторы):**

**А.Л. Соколов, преподаватель ФГБОУ ВО "РЭУ им. Г.В.Плеханова"**
Ф.И.О., ученая степень, звание, должность, наименование ФГБОУ

Лист актуализации

рабочей программы учебной дисциплины

В рабочую программу учебной дисциплины на 2018/19 уч. год внесены следующие изменения:

1. На основании Указа Президента РФ от 15.01.2018 года №215 на титульном листе исправлено Министерство образования и науки Российской Федерации на Министерство науки и высшего образования Российской Федерации

Дата актуализации: 30.08.2018 г

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.16 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 учебной дисциплины в структуре основной профессиональной образовательной программы:** общепрофессиональная дисциплина профессионального цикла

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

В результате освоения учебной дисциплины обучающийся должен

**уметь:**

- выявлять потенциальных нарушителей информационной безопасности;
- производить оценку угроз информации;
- применять алгоритмы криптографии для защиты данных;
- использовать методы и средства защиты данных в зависимости от потенциальных пользователей системы;
- применять методы шифрования организованных структур данных;
- создавать дополнительные средства защиты, опираясь на персональные данные компьютера пользователя;
- пользоваться современными приложениями защиты авторских прав:
- проводить анализ и оценивать механизмы защиты;
- выбирать формы и критерии информационной безопасности;
- использовать средства защиты от вредоносного программного обеспечения;
- разрабатывать предложения по совершенствованию политики безопасности.

**знать**:

- терминологию в сфере безопасности информационного контента;
- понятия политики безопасности, существующие типы политик безопасности;
- существующие стандарты информационной безопасности;
- виды угроз информационной безопасности;
- средства борьбы с угрозами информационной безопасности;
- о современных концепциях безопасности программного обеспечения и баз данных;
- методы защиты информации;
- критерии защищенности программного обеспечения и баз данных;
- угрозы безопасности программного обеспечения и баз данных;
- критерии и методы оценивание механизмов защиты;
- организационно-правовое обеспечение информационной безопасности.

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.
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.

**1.4. Рекомендуемое количество часов на освоение программы дисциплины:**

| | | |
|---|---|---|
| **Максимальная учебная нагрузка обучающего** | 90 | часов |
| Включая: | | |
| Обязательная аудиторная нагрузка | 60 | часов |
| Самостоятельная работа | 28 | часов |
| Консультации | 2 | часа |
| **ВСЕГО** | **90** | **часов** |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

### 2.1. Объем нагрузки учебной дисциплины

| Вид учебной работы | Объем часов |
|---|---|
| **Максимальная учебная нагрузка (всего)** | **90** |
| **Обязательная аудиторная учебная нагрузка (всего)** | **60** |
| в том числе: | |
| практические занятия | 20 |
| **Самостоятельная работа обучающегося** | **28** |
| **Консультации** | **2** |
| **Итоговая аттестация**<br>5 семестр - экзамен | |

**2.2. Тематический план и содержание тем учебной дисциплины ОП.16 Информационная безопасность**

| Наименование разделов и тем | Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся | Объем часов | Уровень освоения |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Раздел 1. Информация как объекта защиты** | | **15** | |
| **Тема 1.1.** Общие сведения о защите информации. | Понятие об опасной информации. Виды опасной информации. Способы защиты человека от излишней, назойливой, недобросовестной информации. Вредная информация в формах обмана и злоупотребления доверием. Ценность информации. | 2 | 1 |
| **Тема 1.2.** Основные понятия и определения**.** | Основные понятия в информационной безопасности. | 2 | 1 |
| | **Самостоятельная работа обучающихся** | 2 | |
| | Национальные интересы и безопасность | | |
| **Тема 1.3.** Базовая модель нарушителя**.** | Структура базовой модели нарушителя. Описание нарушителей (субъектов атак). | 2 | 1 |
| | **Самостоятельная работа обучающихся** | 1 | |
| | Анализ действий нарушителя информационной безопасности предприятия | | |
| **Тема 1.4.** Агенты угроз информационной безопасности. | Информационные нарушители. Цели нарушителей. Оценка опасности нарушителя на основании его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя. | 2 | 1 |
| | **Практическая работа** | 2 | |
| | Оценка угроз и агентов угроз | | |
| | **Самостоятельная работа обучающихся** | 2 | |
| | Элементы и объекты защиты в автоматизированных системах обработки данных | | |
| **Раздел 2. Направления информационной защиты** | | **15** | |
| **Тема 2.1.** Виды мер и основные принципы обеспечения информационной безопасности**.** | Характеристика нормативно-правовой защиты. Виды информации по категории доступа. Правовой режим защиты государственной тайны. Правовой режим защиты конфиденциальной информации. Виды конфиденциальной информации и режимы ее защиты. Ответственность за право нарушения в сфере защиты конфиденциальной информации. | 2 | 1 |
| | **Самостоятельная работа** | 2 | |
| | Проблемы реализации применения основных принципов информационной безопасности | | |
| **Тема 2.2.** Классификация угроз информационной безопасности. | Основные понятия об источниках угроз, факторах и последствиях. Виды проявления ущерба. Классификация угроз информационной безопасности. | 2 | 1 |

| | | | |
|---|---|---|---|
| | Классификация источников угроз. Классификация уязвимостей безопасности. | | |
| **Тема 2.3.** Возможные каналы утечки информации. | Угрозы и возможные каналы утечки конфиденциальной информации. Виды угроз. Предпосылки появления угроз. Обобщенный перечень угроз и перечень мероприятий по защите данных. Рекомендуемые мероприятия по защите. | 2 | 1 |
| | **Самостоятельная работа** | 1 | |
| | Сравнительный анализ возможных каналов утечки информации | | |
| **Тема 2.4.** Правовые основы защиты персональных данных. | Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». Основные понятия в законе. Защита персональных данных работников по Трудовому кодексу РФ. | 2 | 1 |
| **Тема 2.5.** Уголовный кодекс РФ глава 28. Преступления в сфере компьютерной информации | Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 (с изм. и доп. от 07.07.2007).<br>Уголовно-процессуальный кодекс Российской Федерации № 174-ФЗ от 18.12.2001 (с изм. и доп. от 07.07.2003).<br>Кодекс РФ об административных нарушениях № 195-ФЗ от 30.12.2001 (с изм. и доп. от 4.07.2003).<br>Гражданский кодекс РФ. Часть четвертая. ТК Велби, Изд-во Проспект, 2007.<br>ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006.<br>ФЗ «О связи», № 126-ФЗ от 07.07.2003. | 2 | 1 |
| | **Самостоятельная работа** | 2 | |
| | Сравнительный анализ преступлений в сфере компьютерной безопасности в странах ближнего зарубежья. | | |
| **Раздел 3. Методы и средства защиты программного обеспечения** | | **22** | |
| **Тема 3.1.** Методы защиты программного обеспечения. | Аппаратные ключи защиты. Ключи с памятью. Ключи с неизвестным алгоритмом. Ключи с таймером. Ключи с известным алгоритмом. Ключи с программируемым алгоритмом. Программные средства защиты программного обеспечения. Алгоритмы запутывания (обфускация). Метод шифрования программного кода. Метод проверки целостности кода программы. Метод эмуляции процессора. Выполнение на стороне сервера. | 2 | 1 |
| | **Самостоятельная работа** | 1 | |
| | Анализ современного программного обеспечения в области информационной безопасности предприятий и частных лиц. | | |
| **Тема 3.2.** Регистрационные коды для программ. | Требования и классификация. Методы проверки регистрационных кодов. «Черный ящик». Сложная математическая задача. Табличные методы. Выбор метода. | 2 | 1 |
| **Тема 3.3.** Методы и средства | Инструменты динамического исследования ПО. Инструменты статического | 2 | 1 |

| | | | |
|---|---|---|---|
| защиты программ от компьютерных вирусов и средств исследования программ. | исследования ПО. Защита от отладчиков. Защита от эмулирующих отладчиков. Защита от дизассемблеров. | | |
| **Тема 3.4.** Криптография. | Участники взаимодействия. Объекты и операции. Симметричные алгоритмы. Алгоритмы шифрования. Криптографические хэш-функции. Криптографические генераторы псевдослучайных чисел. Модели основных криптоаналитических атак. Атака на основе только шифртекста. Атака на основе открытого текста. Атака на основе подобранного открытого текста.<br>Модели распространения программного обеспечения. Бесплатные программы (Freeware). Почти бесплатные программы. Программы, показывающие рекламу (Adware). Коммерческие программы (Commercial). Почти работоспособные программы. Условно бесплатные продукты (Shareware). | 2 | 1,2 |
| | **Практическая работа** | 6 | |
| | Создание системы защиты ПО, применяя криптографические методы. | | |
| | Модификация системы, разделяя группы пользователей, привилегии, роли и представления информации. | | |
| | XOR-шифрование | | |
| | **Самостоятельная работа** | 7 | |
| | Проблемы реализации методов криптографической защиты в автоматизированных системах обработки данных | | |
| | Актуальные задачи защиты программ | | |
| | Особенности защиты информации в персональных ЭВМ | | |
| **Раздел 4. Механизмы обеспечения информационной безопасности программного обеспечения и баз данных** | | **36** | |
| **Тема 4.1.** Привязка программного обеспечения к аппаратным средствам | Основные способы и виды привязки программного обеспечения к аппаратным средствам. | 2 | 1,2 |
| | **Практическая работа** | 4 | |
| | Аппаратная привязка программного обеспечения | | |
| | Работа с программой WinLicense. | | |
| | **Самостоятельная работа** | 4 | |
| | Цели, функции и задачи защиты информации в сетях ЭВМ | | |
| | Технические средства защиты | | |
| **Тема 4.2.** Шифрование RSA. | Описание алгоритма. История создания. Шифрование и расшифрование. Цифровая подпись. | 2 | 1 |

| | | | |
|---|---|---|---|
| | **Практическая работа** | 4 | |
| | Работа с программой The Enigma Protector. | | |
| | Использование программы VMProtect. | | |
| | **Самостоятельная работа** | 3 | |
| | Достоинства и недостатки программного обеспечения, используемого для защиты данных | | |
| | Вредоносные закладки в ПК и борьба с ними | | |
| **Тема 4.3.** Безопасность web-приложений. | Особенности XSS-атак. Виды SQL-инъекций. Локальные и удаленные инклуды. | 2 | 1 |
| **Тема 4.4.** Компьютерные вирусы. | История. Классификация. Распространение. Механизм. Каналы. Противодействие. | 2 | 1 |
| **Тема 4.5.** Антивирусные средства. | Классификация. Работа антивирусных средств. База. Целевые платформы антивирусных средств. | 2 | 1 |
| | **Практическая работа** | 2 | |
| | Анализ антивирусных продуктов | | |
| | **Самостоятельная работа** | 2 | |
| | Сравнительный анализ современных антивирусных комплексов, используемых в РФ | | |
| **Тема 4.6.** Уязвимость компьютерных сетей | Проблемы безопасности протоколов TCP/IP. Методы и инструменты. Прослушивание сети. Сканирование сети. Генерация пакетов. Перехват данных. Ложные ARP-ответы. Навязывание ложного маршрутизатора. Имперсонация. Несанкционированное подключение к сети. Туннелирование. Атака крошечными фрагментами (Tiny Fragment Attack). Принуждение к ускоренной передаче данных. Отказ в обслуживании. Ложные DHCP-клиенты. | 2 | 1 |
| | **Практическая работа** | 2 | |
| | Анализ уязвимостей компьютерных сетей. | | |
| | **Самостоятельная работа** | 1 | |
| | Архитектура механизмов защиты информации в сетях ЭВМ | | |
| **Тема 4.7.** Защита баз данных. | Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. | 2 | 1 |
| **Консультации** | | **2** | |
| | **Всего:** | **90** | |

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 УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Реализация программы учебной дисциплины требует наличия Лаборатории обработки информации отраслевой направленности

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|---|---|---|---|
| 1 | Парты 17 шт | проектор 1 шт | 22 |
| 2 | стулья 22 шт | компьютер 9 шт | |
| 3 | доска маркерная | | |
| 4 | стол преподавателя 2 шт • | | |
| 5 | кондиционер 1 шт • | | |

**Программное обеспечение:**
Android Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition, Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

### 3.2. Информационное обеспечение обучения

Печатные издания не используются. Дисциплина полностью обеспечена электронными изданиями.

| № п/п | Наименование учебных изданий, Интернет-ресурсов, дополнительной литературы |
|---|---|
| **I** | **Основные источники** |
| 1.1 | Т. Л. Партыка, И. И. Попова «Информационная безопасность» (5-е издание) Москва, Издательство «Форум: НИЦ ИНФРА-М» 2018. Режим доступа: http://www.znanium.com/bookread.php?book=420047 |
| 1.2 | В. Ф. Шаньгин, «Информационная безопасность компьютерных систем и сетей» (учебное пособие) Москва, Издательство «Форум: НИЦ ИНФРА-М» 2014. Режим доступа: http://www.znanium.com/bookread.php?book=335362book=335362 |
| 1.3 | Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2017. Режим доступа: http://http://http://znanium.com/bookread2.php?book=882007 В. Г. Спицын «Информационная безопасность вычислительной техники» (учебное пособие) Томск, Издательство «Эль Контент» 2011. Режим доступа: http://biblioclub.ru/index.php?page=book&id=208694&sr=1 |
| 1.4 | Е.В. Глинская, Н.В. Чичварин Информационная безопасность конструкций ЭВМ и систем. — М. : ИНФРА-М, 2018 Режим доступа: http://znanium.com/bookread2.php?book=925825 |
| **II** | **Дополнительные источники** |
| 2.1 | Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016 Режим доступа: http://znanium.com/bookread2.php?book=544554 |
| 2.2 | Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - М.:Гор. линия-Телеком, 2016 Режим доступа: |

| | |
|---|---|
| | http://znanium.com/bookread2.php?book=973806 |
| 2.3 | В. Ф. Шаньгин «Защита информации в компьютерных системах и сетях» (учебник) Москва, Издательство «ДМК Пресс» 2016. Режим доступа: http://biblioclub.ru/index.php?page=book&id=231889&sr=1 |
| 2.4 | В. И. Аверченков, М. Ю. Рытов «Служба защиты информации: организация и управление» (учебное пособие) Москва, Издательство «Флинта» 2015. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93356&sr=1 |
| **III** | **Электронно библиотечная система (ЭБС)** |
| 3.1 | http://znanium.com/ |
| 3.2 | http://biblioclub.ru |
| 3.3 | https://biblio-online.ru/ |
| 3.4 | https://www.book.ru/ |
| **IV** | **Профессиональные базы данных и справочные системы** |
| 4.1 | Федеральная служба государственной статистики - https://rosstat.gov.ru/ |
| 4.2 | Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com |
| 4.3 | Информационно-справочная система "КонсультантПлюс" |

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Образовательное учреждение, реализующее подготовку по учебной дисциплине, обеспечивает организацию и проведение промежуточной аттестации и текущего контроля индивидуальных образовательных достижений – демонстрируемых обучающимися знаний, умений и навыков.

Текущий контроль проводится преподавателем.

Формы и методы промежуточной аттестации текущего контроля по учебной дисциплине самостоятельно разрабатываются образовательным учреждением и доводятся до сведения обучающихся не позднее начала двух месяцев от начала обучения.

Итоговой формой контроля является экзамен

Фонды оценочных средств (ФОС, КОС) разрабатываются образовательным учреждением. Они включают в себя педагогические контрольно-оценочные материалы, предназначенные для определения соответствия (или несоответствия) индивидуальных образовательных достижений основным показателям результатов подготовки (таблицы).

| **Результаты обучения (освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
|---|---|
| **Умения** | |
| — выявлять потенциальных нарушителей информационной безопасности;<br>— производить оценку угроз информации;<br>— применять алгоритмы криптографии для защиты данных;<br>— использовать методы и средства защиты данных в зависимости от потенциальных пользователей системы;<br>— применять методы шифрования организованных структур данных;<br>— создавать дополнительные средства защиты, опираясь на персональные данные компьютера пользователя;<br>— пользоваться современными приложениями защиты авторских прав:<br>— проводить анализ и оценивать механизмы защиты; | Устный опрос<br>Наблюдение и оценка результата выполнения практических работ<br>Тестирование<br>Внеаудиторная самостоятельная работа<br>Экзамен |

| | |
|---|---|
| — выбирать формы и критерии информационной безопасности;<br>— использовать средства защиты от вредоносного программного обеспечения;<br>— разрабатывать предложения по совершенствованию политики безопасности. | |
| **Знания:** | |
| — терминологию в сфере безопасности информационного контента;<br>— понятия политики безопасности, существующие типы политик безопасности;<br>— существующие стандарты информационной безопасности;<br>— виды угроз информационной безопасности;<br>— средства борьбы с угрозами информационной безопасности;<br>— о современных концепциях безопасности программного обеспечения и баз данных;<br>— методы защиты информации;<br>— критерии защищенности программного обеспечения и баз данных;<br>— угрозы безопасности программного обеспечения и баз данных;<br>— критерии и методы оценивание механизмов защиты;<br>— организационно-правовое обеспечение информационной безопасности. | Устный опрос<br>Наблюдение и оценка результата выполнения практических работ<br>Тестирование<br>Внеаудиторная самостоятельная работа<br>Экзамен |

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

| **Процент результативности (правильных ответов)** | **Качественная оценка индивидуальных образовательных достижений** | |
|---|---|---|
| | **балл (отметка)** | **вербальный аналог** |
| более 90 | 5 | отлично |
| от 70 до 89 | 4 | хорошо |
| от 50 до 69 | 3 | удовлетворительно |
| менее 49 | 2 | неудовлетворительно |

**Разработчики:**
Батенко К.Е., преподаватель ФГБОУ ВО "РЭУ им. Г.В. Плеханова"

**Эксперт:**