

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
Российский экономический университет имени Г.В.Плеханова
Московский приборостроительный техникум

Специальность:
10.02.05 Обеспечение
информационной безопасности
автоматизированных систем
Квалификация:
Техник по защите информации

АННОТАЦИЯ

к рабочей программе профессионального модуля
ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

1. Место дисциплины в структуре основной образовательной программы в структуре ППССЗ

Рабочая программа профессионального модуля (далее — рабочая программа) является частью программы подготовки специалистов среднего звена (ППССЗ), в соответствии с ФГОС по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем (базовой и углубленной подготовки) в части освоения основного профессионального модуля (ПМ): ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

2. Цель изучения дисциплины

Приобретение теоретических знаний, практических умений и навыков в ходе изучения следующих дидактических тем: Предмет и задачи программно-аппаратной защиты информации; Стандарты безопасности; Защищенная автоматизированная система; Дестабилизирующее воздействие на объекты защиты; Принципы программно-аппаратной защиты информации от несанкционированного доступа; Основы защиты автономных автоматизированных систем; Защита программ от излучения; Вредоносное программное обеспечение; Защита программ и данных от несанкционированного копирования; Защита информации на машинных носителях; Аппаратные средства идентификации и аутентификации пользователей; Системы обнаружения атак и вторжений; Основы построения защищенных сетей; Средства организации VPN; Обеспечение безопасности межсетевого взаимодействия; Защита информации в базах данных; Мониторинг систем защиты; Изучение мер защиты информации в информационных системах; Изучение современных программно-аппаратных комплексов; Математические основы криптографии; Методы криптографической защиты информации; Криптоанализ; Поточные шифры и генераторы псевдослучайных чисел; Кодирование информации. Компьютеризация шифрования; Симметричные системы шифрования; Асимметричные системы шифрования; Аутентификация данных. Электронная подпись; Алгоритмы обмена ключей и протоколы аутентификации; Криптозащита информации в сетях передачи данных; Защита информации в электронных платежных системах; Компьютерная стеганография.

3. Структура дисциплины

Профессиональный модуль изучается на 3 и 4 курсах, на протяжении 4 семестров. Изучение дисциплины предполагает освоение материала в объеме максимальной учебной нагрузки обучающегося 831 часов, в том числе: обязательной аудиторной учебной нагрузки обучающегося 831 часа; на освоение МДК — 497 часов, в том числе, на промежуточную аттестацию по МДК — 8 часов, на практики — 324 часов

4. Основные образовательные технологии

Лекции, практические и лабораторные занятия, самостоятельная работа студентов по изучению теоретических вопросов и выполнению практических заданий, тестирование, контрольные работы. В состав профессионального модуля входят 2 МДК и 1 УП и 1 ПП:

- МДК.02.01 Программные и программно-аппаратные средства защиты информации
- МДК.02.02 Криптографические средства защиты информации
- УП.02.01 Учебная практика
- ПП.02.01 Производственная практика

5. Требования к результатам освоения дисциплины

В результате освоения учебной дисциплины обучающийся должен **уметь**:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- применять средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

В результате освоения учебной дисциплины обучающийся должен **знать**:

- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Дисциплина способствует формированию следующих общих компетенций (ОК) и профессиональных компетенций (ПК):

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	<i>Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.</i>
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
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.

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	<i>Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</i>
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

6. Форма контроля

В качестве форм контроля используются:

8-м семестре – Экзамен квалификационный