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

# РАБОЧАЯ ПРОГРАММА

Профессиональный модуль: ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности

| | |
|---|---|
| Код, специальность: | 10.02.03 Информационная безопасность автоматизированных систем |
| Квалификация: | Техник по защите информации |
| Форма обучения: | Очная |

2018

СОГЛАСОВАНА

цикловой методической комиссией

«Профессиональных модулей

10.02.03»

Протокол 01-18/19
от 31 августа 2018 г

Председатель
цикловой методической комиссии

М. С. Прищеп
подпись | инициалы, фамилия

Разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности

**10.02.03 Информационная безопасность автоматизированных систем**

код, наименование специальности

Заместитель директора техникума
по учебной работе

Д. А. Клонов
подпись | инициалы, фамилия

УТВЕРЖДЕНА
Директор техникума

А. В. Чурилов
подпись | инициалы, фамилия

Главный отдел АО «Металлургмаш»
наименование предприятия (организации), должность

СОГЛАСОВАНА
Представитель работодателя

С.Г. Ахмадеев
подпись | инициалы, фамилия

СОДЕРЖАНИЕ

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

# ПМ.03 ПРИМЕНЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.1 Область применения программы

Рабочая программа профессионального модуля (далее — рабочая программа) является частью программы подготовки специалистов среднего звена (ППССЗ), в соответствии с ФГОС по специальности СПО 10.02.03 Информационная безопасность автоматизированных систем». Квалификация: техник по защите информации (базовой и углубленной подготовки) в части освоения основного профессионального модуля (ПМ): **ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности** и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

**1.2. Место профессионального модуля в структуре ППССЗ:**

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

**иметь практический опыт:**

- выявление технических каналов утечки информации;

- использование основных методов и средств инженерно-технической защиты информации;

- диагностики, устранение отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;

- участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

**уметь:**

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;

**знать:**

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализов сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;
- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения

**3. Количество часов на освоение программы профессионального модуля:**

максимальная учебная нагрузка обучающегося - 615 часов, включая:
обязательную аудиторную учебную нагрузку обучающегося - 410 часов;
самостоятельную работу обучающегося - 205 часов;

## 2.. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **Применение инженерно-технических средств обеспечения информационной безопасности**, в том числе профессиональными и общими компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

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.

ОК 10. Формулировать задачи логического характера и применять средства математической логики для их решения.

ОК 11. Владеть основными методами и средствами разработки программного обеспечения.

ОК 12. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.2. Тематический план профессионального модуля

| Код профессиональных компетенций | Наименования разделов профессионального модуля* | Всего часов | Объем времени, отведенный на освоение междисциплинарного курса (курсов) | | | | | Практика | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Обязательная аудиторная учебная нагрузка обучающегося | | | Самостоятельная работа обучающегося | | Учебная, часов | Производственная (по профилю специальности), ** часов |
| | | | Всего, часов | в т.ч. лабораторные работы и практические занятия, часов | в т.ч., курсовая работа (проект), часов | Всего, часов | в т.ч., курсовая работа (проект), часов | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ПК 3.1-3.3 | МДК.03.01Применение инженерно-технических средств обеспечения | 237 | 158 | 80 | | 79 | | | - |
| ПК 3.4-3.5 | МДК.03.02Электрорадиоизмерения и источники питания | 225 | 150 | 58 | | 75 | | | - |
| ПК 3.5 | МДК.03.03Метрология, стандартизация и сертификация | 102 | 68 | 20 | | 34 | | | |
| ПК 3.4-3.5 | МДК.03.04Экономические аспекты проектирования компьютерных систем и защиты информации | 51 | 34 | 10 | | 17 | | | |

## 3.2. Содержание обучения по профессиональному модулю

| Наименование разделов ПМ, МДК и тем | | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) | Объем часов | |
|---|---|---|---|---|
| 1 | | 2 | 3 | |
| **Раздел 1. Применение инженерно-технических средств** | | | | |
| **МДК.03.01. Применение инженерно-технических средств обеспечения информационной безопасности** | | | | |
| **Тема 1.1 Система инженерно-технической защиты информации** | | | **34** | |
| | 1 | Подсистема физической защиты источников информации. Подсистема инженерно-технической защиты информации от ее утечки. Управление силами и средствами системы инженерно-технической защиты информации. Классификация средств инженерно-технической защиты информации | | **2** |
| | 2 | Ограждения территории. Ограждения зданий и сооружений. Металлические шкафы, сейфы и хранилища. Средства систем контроля и управления доступом. Средства обнаружения злоумышленников и пожара. Извещатели. Средства контроля и управления средствами охраны. Средства телевизионной охраны. Средства оповещения. | | **3** |
| | 3 | Средства противодействия наблюдению в различных диапазонах. Средства звукоизоляции и звукопоглощения акустического сигнала. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств. Классификация средств обнаружения и локализации. Аппаратура радиоконтроля. Средства контроля телефонных линий и цепей электропитания. Технические средства подавления сигнала закладных устройств. Средства контроля помещений на отсутствие закладных устройств | | **2** |
| **Тема 1.2 Организационные основы инженерно-технической защиты информации** | | | **20** | |
| | 1 | Задачи и структура государственной системы инженерно-технической защиты информации. Организация инженерно-технической защиты информации на предприятиях, в учреждениях. Нормативно-правовая база инженерно-технической защиты информации | | **2** |
| | 2 | Основные организационные и технические меры по обеспечению инженерно-технической защиты информации. Контроль эффективности инженерно-технической защиты информации | | **3** |
| **Тема 1.3 Методическое** | | | **24** | |
| | 1 | Алгоритм проектирования системы защиты информации. Моделирование объектов защиты. Моделирование угроз информации. Моделирование каналов несанкционированного доступа к информации. Моделирование каналов утечки информации | | **3** |
| | 2 | Организация защиты источников информации при помощи активного оборудования. Выбор технических средств охраны. Типовые меры по защите информации от наблюдения. Типовые меры по защите информации от подслушивания. Типовые меры по защите информации от перехвата | | **2** |
| | **Практические занятия** | | **80** | |
| | 1 | Обоснование выбора кабинета как объекта защиты | | |
| | 2 | Проведение анализа защищаемой в кабинете руководителя информации | | |
| | 3 | Составление плана кабинета как объекта защиты | | |

| | | | | |
|---|---|---|---|---|
| | 4 | Моделирование угроз воздействия на источники информации | | |
| | 5 | Моделирование технических каналов утечки информации | | |
| | 6 | Разработка и осуществление мер по предотвращению проникновения злоумышленника к источникам информации | | |
| | 7 | Осуществление защиты информации в кабинете | | |
| | 8 | Осуществление защиты речевой информации от подслушивания | | |
| | 9 | Предотвращение перехватов радио- и электрических сигналов | | |
| | | **Самостоятельная работа обучающегося**<br>Работа с конспектами лекций, учебной и специальной технической литературой<br>Решение задач<br>Построение подсистем физической защиты информации<br>Применение средств инженерной защиты<br>Применение средств противодействия наблюдению и прослушиванию<br>Осуществление организации инженерно-технической защиты информации<br>Разработка типовых мер по инженерно-технической защите информации<br>Настройка системы защиты операционных систем, способов управления доступом<br>Изучение рекомендаций по моделированию системы инженерно-технической защиты информации<br>Реализация мер инженерно-технической защиты информации | **79** | |
| | | | | |
| **Раздел 2. Электрорадиоизмерения и источники питания** | | | | |
| **МДК.03.02 Электрорадиоизмерения и источники питания** | | | | |

| **Наименование разделов и тем** | **Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект)** *(если предусмотрены)* | **Объем часов** | **Уровень освоения** |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| **Введение** | . | | |
| **Раздел 1** | | **28** | |
| **Тема 1.1** | Содержание учебного материала | | *ознакомительный* |
| | Введение. Характеристика государственной системы противодействия технической разведке; | **2** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| **Тема 1.2** | Содержание учебного материала | | *ознакомительный* |
| | Нормативные документы по противодействию технической разведке. Свойства и виды информации Виды, источники и носители защищаемой информации | **2** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| | Содержание учебного материала | **2** | *ознакомительный* |

| | | | |
|---|---|---|---|
| **Тема 1.3** | Демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники | | |
| | Практическая работа: | **2** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | *продуктивный* |
| **Тема 1.4** | Содержание учебного материала | | *ознакомительный* |
| | Средства и методы технической разведки. Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой | **2** | |
| | Практическая работа:<br>Обнаружение и локализация источников радиоизлучений. | **2** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **12** | |
| **Тема 1.5** | Содержание учебного материала | | *ознакомительный* |
| | Способы и средства перехвата сигналов. Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации | **14** | |
| | Практическая работа:<br>Цифровые диктофоны.<br>Генераторы радиошума и блокираторы источников радиосигналов. | **20** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **12** | *продуктивный* |
| **Раздел 2** | | **34** | |
| **Тема 2.1** | Содержание учебного материала | | *ознакомительный* |
| | Технические каналы утечки информации. Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации | **2** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| **Тема 2.2** | Содержание учебного материала | | *ознакомительный* |
| | Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации | **2** | |
| | Практическая работа: | | |

| | | | |
|---|---|---|---|
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **12** | |
| **Тема 2.3** | Содержание учебного материала | | *ознакомительный* |
| | Электромагнитные каналы утечки информации. Акустические каналы утечки информации | **2** | |
| | Практическая работа:<br>Изучение механизмов акустоэлектрических преобразований<br>Изучения принципа работы и применения лазерного микрофона | **2** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | *продуктивный* |
| **Тема 2.4** | Содержание учебного материала | | *ознакомительный* |
| | Виброакустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации | **2** | |
| | Практическая работа:<br>Обнаружение и локализация закладных устройств с помощью нелинейного локатора.<br>Принципы дозиметрической разведки. Дозиметрия ионизирующих излучений. | **2** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| **Тема 2.5** | Содержание учебного материала | | *ознакомительный* |
| | Средства обнаружения технических каналов утечки информации. Средства обнаружения и локализации закладных устройств. Нелинейные локаторы | | |
| | Практическая работа:<br>Многофункциональные поисковые приборы, программный коррелятор<br>Обнаружение и локализация акустических закладных устройств, программный коррелятор | **12** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **11** | *продуктивный* |
| **Тема 2.6** | Содержание учебного материала | | *ознакомительный* |
| | Сканирующие приёмники. Детекторы электромагнитного поля. Программно-аппаратные автоматизированные комплексы. Досмотровая техника | **2** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |

| | | | |
|---|---|---|---|
| | | | |
| **Тема 2.7** | Содержание учебного материала | | *ознакомительный* |
| | Мероприятия по выявлению средств технической разведки | **4** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | *продуктивный* |
| **Раздел 3** | | **46** | |
| **Тема 3.1** | Содержание учебного материала | | *ознакомительный* |
| | Методы и средства защиты информации от утечки по техническим каналам. Пассивные и активные методы защиты | **14** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| **Тема 3.2** | Содержание учебного материала | | *ознакомительный* |
| | Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов | **14** | |
| | Практическая работа:<br>Многофункциональные поисковые приборы | **12** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |
| **Тема 3.3** | Содержание учебного материала | | *ознакомительный* |
| | Обнаружение и локализация закладных устройств, подавление их сигналов; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания | **14** | |
| | Практическая работа:<br>Многофункциональные поисковые приборы | **4** | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | *продуктивный* |
| **Тема 3.4** | Содержание учебного материала | | *ознакомительный* |
| | Концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов | | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |

| | | | |
|---|---|---|---|
| **Тема 3.5** | Содержание учебного материала | | *ознакомительный* |
| | Виды контроля эффективности защиты информации; физические принципы контроля защиты информации; основные положения методологии инженерно-технической защиты информации | **6** | |
| | Практическая работа:<br>Универсальный анализатор проводных линий<br>Многофункциональные поисковые приборы | **4** | |
| | Самостоятельная работа обучающихся:<br>1. | **2** | *продуктивный* |
| **Тема 3.6** | Содержание учебного материала | | *ознакомительный* |
| | Методы расчета и инструментального контроля показателей защиты информации. Средства измерения при инструментальном контроле | **6** | |
| | Практическая работа: | | |
| | Самостоятельная работа обучающихся:<br>1. Работа с учебной литературой | **2** | |

| | | | | |
|---|---|---|---|---|
| **Раздел 4. Метрология, стандартизация и сертификация** | | | | |
| **МДК.03.03. Метрология, стандартизация и сертификация** | | | | |
| **Введение** | | | | **2** |
| **Тема 4.1 Законодательная и** | | | **8** | |
| | 1 | Общие сведения о защите конфиденциальных документов<br>Основные документы. Классификация информации. Структура защищаемых документопотоков. Подготовка и издание конфиденциальных исходящих документов. Классификации информации по уровням требований к ее защищенности. Правовое регулирование. Понятие персональных данных. Работа кадровой службы с персональными данными. Общие требования при обработке персональных данных работника и гарантии их защиты. Передача персональных данных работников. Ответственность за нарушение правил | | **3** |
| | | работы с персональными данными. Уголовная ответственность. Административная ответственность. Дисциплинарная ответственность | | |
| **Тема 4.2 Учет конфиденциальных документов и порядок их рассмотрения и исполнения** | | | **8** | |
| | 1 | Размножение конфиденциальных документов. Контроль исполнения конфиденциальных документов. Формирование и хранение дел, содержащих конфиденциальные документы. Выдача и возврат конфиденциальных документов. Проверка наличия конфиденциальных документов. Уничтожение конфиденциальных документов. Подготовка документов к архивному хранению. Оформление дел для сдачи в архив | | **3** |

| | | | | |
|---|---|---|---|---|
| **Тема 4.3 Состав конфиденциальных документов и организация работ по защите конфиденциальной информации** | | | **8** | |
| | 1 | Положение о конфиденциальной информации в электронном виде. Метки документов. Хранение информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии. Создание системы защиты конфиденциальной информации. Устав организации по защите конфиденциальной информации. Раздел «Права и обязанности». Раздел «Конфиденциальная информация». Коллективный договор организации. Раздел «Предмет договора». Раздел «Кадры. Обеспечение дисциплины труда». Раздел «Порядок приема и увольнения рабочих и служащих». Раздел «Основные обязанности рабочих и служащих». Раздел «Основные обязанности администрации». Раздел «Условия конфиденциальности». Организационная защита конфиденциальной информации. Защита информации в компьютерах | | **2** |
| **Тема 4.4 Основы обеспечения сохранности документов** | | | **8** | |
| | 1 | Создание оптимальных условий хранения документов. Стеллажное оборудование. Упаковка документов. Физико-химические факторы разрушения документов. Биологические факторы разрушения документов. Санитарно-гигиенические условия сохранности документов. Температурный режим сохранности документов | | **3** |
| **Тема 4.5 Автоматизированные системы управления документооборота и современные технологии защиты от утечки конфиденциальной информации** | | | **6** | |
| | 1 | Основные концепции безбумажной технологии управления. Системы управления документами. Общие требования к системе документооборота. Классификация СУД. Функции и задачи «Систем Управления Документами». Электронный архив предприятия. Организация хранения электронных документов. Организация учета бумажных и микрографических документов. Организация поиска документов. Поддержка защиты документов от несанкционированного доступа и аудита работы. Каналы утечки конфиденциальной информации. Изолированная автоматизированная система для работы с конфиденциальной информацией. Системы активного мониторинга рабочих станций пользователей. Выделенный сегмент терминального доступа к конфиденциальной информации. Средства контентного анализа исходящих пакетов данных. Средства криптографической защиты конфиденциальной информации | | **3** |
| | **Практические занятия** | | **20** | |
| | 1 | Разработка инструкции по обработке и хранению конфиденциальных документов фирмы | | |
| | 2 | Разработка схемы установки терминального сервера доступа к конфиденциальным данным | | |
| | 3 | Разработка выделенной изолированной АС, предназначенной для обработки конфиденциальной информации | | |
| | 4 | Выявление каналов утечки конфиденциальной информации | | |
| | 5 | Построение системы управления документами | | |
| | 6 | Настройка защиты информации в компьютерах | | |

| | | | | |
|---|---|---|---|---|
| | | **Самостоятельная работа обучающегося**<br>Работа с конспектами занятий, учебной и специальной технической литературой<br>Решение задач распределенной обработки данных<br>Выполнение работ по обработке и хранению документов<br>Разработка состава технологических этапов<br>Выполнение операций по работе с конфиденциальными документами<br>Организация порядка учета конфиденциальных документов<br>Изучение требований обеспечения безопасности и защиты информации<br>Разработка требований к помещению архива<br>Настройка электрического и противопожарного оборудования архивохранилищ<br>Решение проблем организации электронного документооборота | **34** | |
| **Раздел 4 Экономические аспекты проектирования компьютерных систем и защиты информации** | | | | |
| **МДК.03.04Экономические аспекты проектирования компьютерных систем и защиты информации** | | | **24** | |

| | | | |
|---|---|---|---|
| **Экономические аспекты проектирования компьютерных систем и защиты информации** | 1 | Структура ЭИС и их классификация.<br>Понятие обеспечивающих и функциональных подсистем ЭИС и их классификация.<br>Характеристики MRP - ERP-систем.<br>Базовые модели жизненного цикла ЭИС.<br>Основные критерии выбора функционального ППП для ЭИС.<br>Особенности автоматизированных банковских систем.<br>Особенности автоматизации логистической деятельности.<br>Информационные системы стратегического и финансового менеджмента.<br>Раскрыть понятие архитектуры вычислительной системы. Основные элементы архитектуры.<br>Комплексные информационные системы, состав подсистем, классификация.<br>Основные уровни обеспечения информационной безопасности.<br>Основные сервисы программных средств защиты информации в ИС.<br>Иерархия памяти в вычислительной системе (внешняя, оперативная, кэш, местная память (внутренние регистры процессора). Концепция виртуального адресного пространства.<br>Физическая и виртуальная памяти, доступные процессу.<br>Сервисы безопасности для реализации функций защиты в сети.<br>Основные серии стандартов, используемые в РФ в сфере ИТ и АС.<br>Назначение стандартов серии ИСО 9000-14000.<br>Содержание стандарта ISO/IEC 12207 "Информационные технологии - жизненный цикл программного обеспечения".<br>Состав вспомогательных процессов при разработке ПО.<br>Состав стадий и этапов канонического проектирования информационных систем.<br>Содержание работ предпроектного обследования предметной области.<br>Содержание работ проектной стадии.<br>Проектирование процессов обработки информации.<br>Проектирование процессов обработки данных в пакетном режиме.<br>Проектирование процессов обработки данных в диалоговом режиме.<br>Содержание функционально-ориентированного проектирования ИС.<br>Содержание объектно-ориентированного проектирования ИС.<br>Управление памятью в вычислительных системах. Сегментная организация памяти.<br>Страничная организация памяти.<br>Понятие и содержание прототипного проектирования ИС.<br>Технологии параметрически-ориентированного и модельно-ориентированного проектирования.<br>Методы планирования и управления проектами ИС и ресурсами.<br>Проектирование приложений на основе хранилищ данных.<br>Проектирование клиент-серверных информационных систем.<br>Назначение, архитектура экспертных систем.<br>Интеллектуальные информационные системы, классификация.<br>Методы интеллектуального анализа данных в экономике.<br>Механизмы защиты процессов в вычислительных системах: кольца защиты и уровни привилегий.<br>Способы представления знаний в экспертных системах. Особенности экспертных систем на<br>методология их построения. | **2** |

| | | | |
|---|---|---|---|
| | **Практические занятия** | **2** | |
| | Этапы создания экспертных систем общая методология их построения.<br>Генетические алгоритмы в искусственных интеллектуальных системах.<br>Интеллектуальные мультиагентные системы. Понятие и характеристики интеллектуальных агентов.<br>Криптографические методы защиты информации.<br>Классификация угроз информационной безопасности, методы защиты.<br>Основные задачи, решаемые протоколами сетевого уровня модели OSI. Особенности технологий сетей с коммутацией каналов и с коммутацией пакетов.<br>Базы данных и системы управления базами данных, архитектура, классификация. | 10 | **2** |
| | **Самостоятельная работа обучающегося**<br>Виды деятельности для процесса разработки ПО.<br>Классификация программ-вирусов.<br>Технология проектирования ИС на основе объектного подхода.<br>Классификация компьютерных сетей. Отличительные признаки, краткие характеристики.<br>Центральный процессор, назначение и основные функциональные элементы.<br>Модификация адресов в ЭВМ. Назначение индексных, базовых (сегментных) регистров.<br>Концепция системной шины. Назначение адресной шины, шины данных и шины управления.<br>Понятие стека в вычислительной системе. Использование стека при вызове подпрограмм и обработке прерываний.<br>Подсистема прерываний. Организация и назначение. Вектор прерывания. Аппаратный механизм прерываний.<br>Подсистема ввода-вывода. Адресация внешних устройств. Адресное пространство портов ввода-вывода.<br>Сущность методов продвижения пакетов в составных сетях (дейтаграммный метод, логическое соединение, метод виртуального канала). | **17** | |

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы модуля предполагает наличие

- Лаборатории инженерно-технических средств обеспечения информационной безопасности

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|---|---|---|---|
| 1 | Стол преподавателя 1 шт | проектор 1 шт | 32 |
| 2 | парты 21 шт | | |
| 3 | стулья 32 шт | | |
| 4 | шкафы 12 шт | | |
| 5 | автоматизированные рабочие места 11 шт | | |

**Программное обеспечение:**

Androind 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

- Лаборатории электроники и схемотехники

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|---|---|---|---|
| 1 | парты 16 шт | Проектор | 29 |
| 2 | стулья 29 шт | | |
| 3 | стол преподавателя 1шт | | |
| 4 | доска маркерная | | |
| 5 | шкаф 4 шт | | |
| 6 | 8 автоматизированных рабочих мест учащихся | | |

**Программное обеспечение:**

Androind 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

- Кабинета метрологии и стандартизации

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|---|---|---|---|
| 1 | Парты - 14 шт | монитор - 1 шт | 25 |
| 2 | стулья - 25 шт | системный блок - 1 шт | |
| 3 | стол преподавателя - 1 шт | мышь - 1 | |
| 4 | доска маркерная - 1 шт | клавиатура - 1 шт | |
| 5 | | телевизор -1 шт | |

**Программное обеспечение:**

Windows 10 pro, Microsoft Office, Mozila Firefox, Google Chrome, 7-zip, K-Lite Codec Pack

- Лаборатория аппаратных средств вычислительной техники

| № п/п | Оборудование | Технические средства обучения | Количество |
|---|---|---|---|

| | | | рабочих мест |
|---|---|---|---|
| 1 | парта 16 шт | проектор | 29 |
| 2 | стул 29 шт | экран для проектора | |
| 3 | Стол преподавателя | | |
| 4 | 8 автоматизированных рабочих мест учащихся | | |
| 5 | шкаф 4 шт | | |
| 6 | кондиционер 2 шт | | |

**Программное обеспечение**:
Androind 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

**4.2. Информационное обеспечение обучения**

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

Основные источники:


1. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/763644
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с. — (Профессиональное образование). - ISBN 978-5-8199-0331-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/775200


Дополнительные источники:


1. Мартишин, С. А. Базы данных. Практическое применение СУБД SQL и NoSQL-типа для проектирования информационных систем: учебное пособие / С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 368 с. — (Высшее образование). - ISBN 978-5-8199-0660-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/905531
2. А.И. Болдырев, И.В. Василевский, С.Е. Сталенков Методические рекомендации по поиску и нейтрализации средств негласного съема информации: практическое пособие – М.: 2013 г.
3. Гришина, Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-007-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/612572.


**Интернет-ресурсы:**

1. http://wm-help.net/books-online/book/98618/98618-7.html - принципы защиты операционных систем
2. http://rudocs.exdat.com/docs/index-56877.html - принципы построения операционных систем
3. http://www.winblog.ru/2006/08/21/21080608.html - система парольной защиты

4. http://emanual.ru/download/6661.html - средства безопасности для защиты сервисов
5. http://all-light.narod.ru/apzci/4.htm - механизмы защиты операционных систем
6. http://www.supermegayo.ru/vlomprogr/3.html - Атаки на программное обеспечение.
7. http://www.xnets.ru/plugins/content/content.php?content.113.3 - Сите безопасности Windows
8. http://pmn.narod.ru/secur/audit/ia.htm - идентификация и аутентификация
9. http://kunegin.narod.ru/ref1/dns/glav_10.htm - Защита DNS
10. http://mitilan.blogspot.ru/2010/03/solaris-10_15.html - Реализация базовых функций по обеспечению безопасности Solaris.
11. http://asher.ru/security/book/its/08 - приемы обеспечения безопасности информационных систем.
12. http://motchim.at.ua/news/tekhnicheskie_kanaly_utechki_informacii_i_ikh_klassifikacija/2009-12-26-23 - Структура, характеристики и классификация технических каналов утечки информации.
16. http://www.bnti.ru/showart.asp?aid=660&lvl=03.03. - Технические каналы утечки информации при передаче ее по каналам связи.
17. http://www.bnti.ru/showart.asp?aid=957&lvl=03. - Технические каналы утечки речевой информации.

**Профессиональные базы данных и справочные системы**

18. Федеральная служба государственной статистики - https://rosstat.gov.ru/
19. Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
20. Информационно-справочная система "КонсультантПлюс"
21.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности. | составление спецификации необходимых инженерно-технических средств обеспечения информационной безопасности объекта; планирование мероприятий по организации обеспечения информационной безопасности объекта; установка, настройка и применение инженерно-технических средств обеспечения информационной безопасности объекта; соблюдение правил применения средств обеспечения информационной безопасности объекта; проведение диагностики работоспособности средств обеспечения информационной безопасности объекта. | Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы:<br>- при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов и т.д.;<br>- при выполнении и защите практических и лабораторных работ;<br>- при выполнении работ на различных этапах производственной практики;<br>- при проведении тестирования, зачета по МДК, экзамена (квалификационного) по модулю. |
| ПК 3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности,в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении | составление графика проверки работоспособности инженерно-технических средств обеспечения информационной безопасности объекта; планирование текущего ремонта инженерно-технических средств информационной безопасности объекта; проверка режимов эксплуатации средств обеспечения информационной безопасности объекта | |

| | | |
|---|---|---|
| работоспособности. | проведение технического обслуживания средств обеспечения информационной безопасности объекта; определение причин отказов оборудования и выполнение ремонтных работ. | |
| ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности. | выполнение оценки эффективности проводимых мероприятий по защите информации; разработка технологии проведения мониторинга эффективности технических средств информационной безопасности объекта. | |
| ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств. | разработка технологических карт проверки технических средств защиты информации; проведение аттестации объекта защиты; устранение неисправностей, выявленных в результате проверки технических средств системы. | |
| ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами. | обеспечение информационной безопасности инженерно-техническими средствами в соответствии с правильным применением нормативных и правовых актов; разработка локальных нормативных правовых актов для обеспечения организации защиты информации в рамках определенного объекта. | |

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их способности.

| **Результаты (освоенные** | **Основные показатели оценки** | **Формы и методы** |
|---|---|---|

| общие компетенции) | результата | контроля и оценки |
|---|---|---|
| ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. | - проявление интереса к будущей профессии, активности и инициативности в получении профессионального опыта, умений и знаний;<br>-аргументированность и полнота объяснения сущности и социальной значимости будущей профессии;<br>- наличие положительных отзывов по итогам производственной практики;<br>- участие в студенческих конференциях, конкурсах и т.п. | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. | - демонстрация умений планировать собственную деятельность и прогнозировать её результаты;<br>- обоснованность выбора методов и способов действий;<br>- проявление способности коррекции собственной деятельности;<br>- адекватность оценки качества и эффективности собственных действий | |
| ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. | - демонстрация способности решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях | |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. | - рациональность выбора источников информации для эффективного выполнения поставленных задач профессионального и личностного развития;<br>- демонстрация умения осуществлять поиск, анализ и оценку информации с использованием различных источников и информационно-коммуникационных технологий<br>-адекватность оценки полученной информации с позиций её своевременности и достаточности для эффек- | - наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики |

| | | |
|---|---|---|
| | тивного выполнения задач профессионального и личностного развития | |
| ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. | - демонстрация умения осуществлять поиск информации с использованием различных источников и информационно-коммуникационных технологий; | - наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики;<br>- экспертная оценка портфолио работ студента |
| ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. | - демонстрация способности эффективно общаться с преподавателями, сотрудниками, студентами, представителями работодателя | - наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики;<br>- экспертная оценка портфолио работ студента |
| ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. | - демонстрация способности ставить цели, мотивировать и организовывать деятельность членов команды<br>- проявление ответственности за результаты выполнения заданий каждым членом команды;<br>- проявление способности оказать и принять взаимную помощь | - наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики;<br>- экспертная оценка портфолио работ студента |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. | - демонстрация стремления к постоянному профессиональному и личностному росту;<br>- проявление способности осознанно планировать и самостоятельно проводить повышение своей квалификации | - наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики;<br>- экспертная оценка портфолио работ студента |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | - демонстрация умения осваивать новые программные и аппаратные средства защиты информации | - наблюдение и оценка на практических занятиях, в процессе учебной /производственной практики |
| ОК 10. Формулировать задачи логического характера и применять средства математической логики для их решения. | - демонстрация способности формулировать задачи логического характера и применять для их решения средства математической логики | - интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения |

| | | |
|---|---|---|
| | | образовательной программы<br>экспертная оценка на военных сборах |
| ОК 11. Владеть основными методами и средствами разработки программного обеспечения. | демонстрация способности формулировать задачи логического характера и применять для их решения средства математической логики | наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики |
| ОК 12. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах. | демонстрация умения применять основные методы и средства разработки программного обеспечения. | наблюдение и оценка на практических занятиях, в процессе учебной/производственной практики |