



Аннотация рабочей программы дисциплины

ЕН.02. Информатика

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Информатика» принадлежит к циклу базовых дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение содержания учебной дисциплины «Информатика» обеспечивает

достижение студентами следующих результатов:

межпредметном уровне;

– применение навыков сотрудничества со сверстниками, детьми младшего возраста, взрослыми в процессе речевого общения, образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;

– овладение нормами речевого поведения в различных ситуациях межличностного и межкультурного общения;

– готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

– умение извлекать необходимую информацию из различных источников:

– учебно-научных текстов, справочной литературы, средств

массовой информации, информационных и коммуникационных технологий для решения когнитивных, коммуникативных и организационных задач в процессе изучения информатики;

предметных:

- выполнять расчеты с использованием прикладных компьютерных программ;
- использовать сеть Интернет и ее возможности для организации оперативного обмена информацией;
- использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;
- обрабатывать и анализировать информацию с применением программных средств и вычислительной техники;
- получать информацию в локальных и глобальных компьютерных сетях;
- применять графические редакторы для создания и редактирования изображений;
- применять компьютерные программы для поиска информации, составления и оформления документов и презентаций

В результате освоения дисциплины обучающийся должен знать:

- базовые системные программные продукты и пакеты прикладных программ;
- основные положения и принципы построения системы обработки и передачи информации;
- устройство компьютерных сетей и сетевых технологий обработки и передачи информации;
- методы и приемы обеспечения информационной безопасности;
- методы и средства сбора, обработки, хранения, передачи и накопления информации;
- общий состав и структуру персональных электронно-вычислительных машин (ЭВМ) и вычислительных систем;
- основные принципы, методы и свойства информационных и телекоммуникационных технологий, их эффективность.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальная учебная нагрузка студентов 64 часа, в том числе:

- обязательной аудиторной учебной нагрузки студентов 48 часов (в том числе практических работ 30 часов);
- самостоятельной работы студентов 16 часов.

Форма контроля: 3 семестр – экзамен.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Информационная деятельность человека. Этапы развития информационного общества. Этапы развития технических средств и информационных ресурсов. Информационные ресурсы общества. Виды профессиональной информационной деятельности человека с использованием технических средств. Правовые нормы, относящиеся к информации.

Раздел 2. Информация и информационные процессы. Основные подходы к понятию «информация». Виды и свойства информации. Измерение информации. Кодирование информации. Системы счисления, используемые в ПК. Принципы обработки информации компьютером. Арифметические основы работы компьютера. Алгебра логики. Понятие об алгоритме, свойства, способы записи. Носитель информации: понятие, виды, основная характеристика. Способы записи информации: магнитный и оптический. Архив информации: понятие, виды, основные характеристика. Определение объёма различных носителей информации. Поиск информации, хранящейся на компьютере. Программные поисковые сервисы. Организация поиска путём использования ключевых слов и фраз. Передача информации посредством каналов связи, их основная характеристика. Характеристика организации проводной связи между компьютерами. Характеристика организации беспроводной связи между компьютерами. Электронная почта. Информационно-поисковые системы и средства работы с ними.

Раздел 3. Средства информационных и коммуникационных технологий. Архитектура ПК, характеристика основных устройств. Магистрально-модульный принцип построения компьютера. Периферийные устройства ПК: виды, основная характеристика. Примеры комплектации компьютера по профилю специальности. Программное обеспечение ПК: виды, характеристика. Понятие локальной сети. Виды, способы организации, основная характеристика ЛС. Программное обеспечение ЛС. Эксплуатационные требования к компьютерному рабочему месту. Защита информации, антивирусная защита.

Раздел 4. Технологии создания и преобразования информационных объектов. Текст как информационный объект: характерные особенности, назначение. Преобразование текста с помощью текстового редактора: редактирование, форматирование, построение таблиц, графических изображений. Структурные элементы текста, их характеристика. ЭТ как информационный объект: характерные особенности, назначение. Основные возможности ЭТ: ввод, редактирование данных. Форматы, проведение математических расчётов, использование функций, построение диаграмм и графиков. Применение ЭТ для решения профессиональных задач. Понятие БД, СУБД как информационной системы. Структурные элементы, виды БД. Этапы создания БД (разбор конкретных примеров). Основные возможности СУБД (на примере Access). Способы представления графической информации: растровая графика, векторная графика, фрактальная графика.

Профессиональная графика по профилю специальности. Понятие мультимедиа. Программная реализация задач мультимедиа. Представление графической и мультимедийной информации с помощью компьютерных презентаций (на примере Р.Point).

Раздел 5. Телекоммуникационные технологии. Технические и программные средства Интернет - технологии: основные понятия, способы и скоростные характеристики подключения, ресурсы Интернет. Провайдер. Использование Интернет - технологии в профессиональной деятельности. Понятие сайта. Способы создания сайта. Основные критерии создания веб – ресурсов. Основные этапы создания сайта, их характеристика. Понятие навигации сайта. Виды навигации. Основные элементы веб – ресурса: баннер, его основная задача, технические характеристики. Другие средства для привлечения пользователей. Виды сервисных услуг глобальной сети Интернет: WWW - E-mail - Usenet - FTP – ICQ- Telnet Характерные особенности телеконференций, Интернет – телефонии. Использование тестирующих систем в учебной деятельности в локальной сети учебного заведения.

Разработчик (и) рабочей программы:

Максимова В.В., преподаватель



Аннотация рабочей программы дисциплины

ОГСЭ.05 Основы финансовой грамотности и предпринимательства

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Основы финансовой грамотности и предпринимательства» принадлежит к циклу общих гуманитарных и социально-экономических дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение содержания учебной дисциплины «Основы финансовой грамотности и предпринимательства» обеспечивает достижение студентами следующих результатов:

В результате изучения учебной дисциплины обучающийся должен уметь:

- решать практические финансовые задачи, анализировать и интерпретировать их условия;
- ставить финансовые цели и планировать деятельность по достижению целей с учётом возможных альтернатив;
- оценивать способы решения практических финансовых задач и делать оптимальный выбор, выполнять самоанализ полученного результата.

В результате изучения учебной дисциплины обучающийся должен знать:

- и владеть базовыми понятиями финансовой сферы (банк, инвестиции, страховой случай, налоги, финансовые риски и др.);

- правила грамотного и безопасного поведения при взаимодействии с финансовыми институтами (банки, фондовый рынок, налоговая служба, страховые компании).

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 40 часов, в том числе:

– обязательная аудиторная учебная нагрузка (всего) 28 часов, из них практическая работа –14 часов.

– самостоятельная работа – 12 часов.

Форма контроля: 5 семестр – дифференцированный зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1 Личные финансы Доходы и расходы личного бюджета. Техника ведения личного бюджета. Финансовое планирование личного бюджета. Обязательное пенсионное страхование. Добровольное пенсионное обеспечение

Раздел 2. Финансы и рынок. Банковская система России. Услуги банков. Облигации. Акции. Фондовая биржа. Страхование. Сущность предпринимательской деятельности. Бизнес-план. Взаимоотношения работодателя и сотрудников. Эффективность компании, банкротство и безработица. Сущность и виды налогов

Разработчик (и) рабочей программы:

Кемадингар Т.В., к.э.н., доцент



Аннотация рабочей программы дисциплины

ОП.01 Основы информационной безопасности

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Основы информационной безопасности» принадлежит к циклу общепрофессиональных дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;

- классифицировать основные угрозы безопасности информации.

В результате освоения дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;

- место информационной безопасности в системе национальной безопасности страны;

- виды, источники и носители защищаемой информации;

- источники угроз безопасности информации и меры по их предотвращению;

- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

- современные средства и способы обеспечения информационной безопасности;

– основные методики анализа угроз и рисков информационной безопасности.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальная учебная нагрузка студентов 48 часов, в том числе:

- обязательной аудиторной учебной нагрузки студентов 48 часов (в том числе практических работ 28 часов);

Форма контроля: 3 семестр – зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Теоретические основы информационной безопасности. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Цели и задачи защиты информации. Основные понятия в области защиты информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности. Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.

Раздел 2. Методология защиты информации. Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации. Организационная структура системы защиты информации. 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. **Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита**

информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.

Разработчик (и) рабочей программы:
Максимова В.В., преподаватель



Аннотация рабочей программы дисциплины

ОП.02 Организационно-правовое обеспечение информационной безопасности

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Организационно-правовое обеспечение информационной безопасности» принадлежит к циклу общепрофессиональных дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ- ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен уметь:

- осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации;
- выявлять каналы утечки информации на объекте защиты;
- контролировать соблюдение персоналом требований режима защиты информации;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- защищать свои права в соответствии с трудовым законодательством;

В результате освоения дисциплины обучающийся должен знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной
- службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- организацию ремонтного обслуживания аппаратуры и средств защиты информации;
- принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;
- правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность)

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 118 часа, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 102 часов, из них практическая работа – 64 часов.
 - самостоятельная работа обучающегося (всего) 16 часа.
- Форма контроля: 5 семестр – экзамен.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Информация как объект правового регулирования. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации. Виды защищаемой информации. Правонарушения в области обеспечения информационной безопасности. Государственная система защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.

Раздел 2. Государственная тайна как особый вид защищаемой информации. Правовой режим защиты государственной тайны. Правовые режимы защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну. Правовой режим обеспечения безопасности персональных данных. Лицензионная и сертификационная деятельности в области защиты информации. Правовые основы защиты информации с использованием технических средств. Защита интеллектуальной собственности средствами патентного и авторского права.

Раздел 3. Международное законодательство в области защиты информации. Система управления (менеджмента) информационной безопасности.

Разработчик (и) рабочей программы:
Ноговицын А.А., преподаватель



Аннотация рабочей программы дисциплины

ОП.03 Основы алгоритмизации и программирования

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Основы алгоритмизации и программирования» принадлежит к циклу общепрофессиональных дисциплин.

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ- ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

- работать в среде программирования;
- использовать языки программирования высокого уровня.

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

- типы данных;
- базовые конструкции изучаемых языков программирования;
- интегрированные среды программирования на изучаемых языках.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 154 часов, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 140 часа;
- самостоятельная работа обучающегося (всего) 8 часов. Форма

контроля: 4 семестр – экзамен.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные принципы алгоритмизации и программирования.

Понятие алгоритма и его свойства. Типы алгоритмов. Способы описания алгоритмов. Базовые алгоритмические структуры: линейные, разветвляющиеся, циклические. Основные базовые типы данных и их характеристика. Основы алгебры логики. Логические операции и логические функции. Принципы построения алгоритмов: использование базовых структур, метод последовательной детализации, сборочный метод. Разработка алгоритмов сложной структуры. Классификация языков программирования. Понятие интегрированной среды программирования. Способы классификации систем программирования. Перечень и назначение модулей системы программирования. Этапы разработки программ: системный анализ, алгоритмизация, программирование, отладка, сопровождение. Характеристика и задачи каждого этапа. Принципы структурного программирования: использование базовых структур, декомпозиция базовых структур. Понятия основных элементов ООП: объекты, классы, методы. Свойства ООП: наследование, инкапсуляция, полиморфизм. Принципы модульного программирования. Понятие отладки. Понятие тестового контроля и набора тестов. Проверка граничных условий, ветвей алгоритма, ошибочных исходных данных. Функциональное и структурное тестирование.

Раздел 2. Язык программирования. История и особенности языка. Области применения. Характеристика системы программирования. Процесс трансляции и выполнения программы. Алфавит и лексика языка. Структура программы. Типы данных языка программирования. Переменные и их описания. Операции с переменными и константами. Правила записи выражений и операций. Организация ввода/вывода данных. Организация ветвлений. Операторы циклов (с предусловием, с постусловием, с параметром). Операторы передачи управления. Одномерные и многомерные массивы, их формирование, сортировка, обработка. Указатели и операции над ними. Определение процедур и функций. Области видимости. Глобальные и локальные переменные. Обращение к процедурам и функциям. Файловый ввод/вывод. Организация обмена данными между программой и внешними устройствами компьютера. Ввод и вывод текстовой информации. Неформатированный ввод/вывод данных. Дополнительные операции с файлами.

Разработчик (и) рабочей программы:

Новиков П.Л., преподаватель



**Аннотация
рабочей программы дисциплины (профессионального модуля,
практики)**

ОП.04 Электроника и схемотехника

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Электроника и схемотехника» принадлежит к циклу общепрофессиональных дисциплин..

**3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-
ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ
ДИСЦИПЛИНЫ**

В результате освоения дисциплины обучающийся должен уметь:

- читать электрические принципиальные схемы типовых устройств электронной техники;
- выполнять расчет и подбор элементов типовых электронных приборов и устройств;
- проводить измерения параметров электрических величин.

В результате освоения дисциплины обучающийся должен знать:

- элементную базу, компоненты и принципы работы типовых электронных приборов и устройств;
- элементную базу, принципы работы типовых цифровых устройств;
- основные сведения об измерении электрических величин;
- принцип действия основных типов электроизмерительных приборов;
- типовые узлы и устройства микропроцессорных систем, микроконтроллеров.

**4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ
ПРОГРАММЫ ДИСЦИПЛИНЫ**

Максимальной учебной нагрузки обучающегося 114 часа, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 114 часов;

– Форма контроля: 5 семестр – зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Электроника. Понятие электрической цепи. Ток, напряжение, ЭДС, мощность в электрической цепи. Схемы электрических цепей. Основные элементы электрических цепей и их параметры.

Закон Ома. Законы Кирхгофа. Баланс мощностей в электрической цепи.

Классификация методов расчета электрических цепей. Современное программное обеспечение для расчета электрических цепей на ЭВМ. Метод преобразования. Метод непосредственного применения законов Кирхгофа.

Основные понятия о синусоидальных электрических величинах. Цепь синусоидального тока с одним элементом (R, L, или C).

Методы расчета цепей синусоидального тока. Расчет электрических цепей синусоидального тока при последовательном соединении элементов. Расчет электрических цепей синусоидального тока при параллельном соединении элементов.

Основные понятия и определения теории переходных процессов. Законы коммутации. Классический метод расчета переходных процессов. Постоянная времени цепи. Основные понятия и определения. Погрешности измерений и их классификация. Средства измерений и их свойства.

Принцип действия основных типов аналоговых приборов. Принцип действия основных типов цифровых приборов.

Общая характеристика методов измерения параметров электрических цепей и устройств. Компенсационный и мостовой методы измерения. Классификация электронных приборов. Собственная и примесная проводимости полупроводников. Физические процессы в свободном p-n-переходе.

Прямое и обратное смещение p-n-перехода. Выпрямительные диоды. Стабилитроны.

Назначение и классификация биполярных транзисторов (БТ). Схемы включения биполярных транзисторов. Физические процессы в БТ.

Статические характеристики БТ в схемах ОЭ и ОБ. Первичные (физические) параметры БТ. Вторичные (h-параметры) БТ.

Динамические характеристики по постоянному току. Динамические характеристики по переменному току.

Полевой транзистор с управляющим p-n-переходом. МДП-транзистор с встроенным каналом. МДП-транзистор с индуцированным каналом.

Классификация электронных усилителей. Структурная схема усилителя и его основные показатели. Принципиальная электрическая схема усилителя. Обеспечение режима работы транзистора в схеме усилителя.

Раздел 2. Схемотехника. Базовые схемные конфигурации аналоговых микросхем. Базовые схемные конфигурации цифровых микросхем. (ТТЛ с простым и сложным инвертором). Особенности построения и виды интегральных усилителей.

Структурная схема операционного усилителя и его основные

показатели. Усилитель с инвертированным входного сигнала. Усилитель без инвертирования входного сигнала.

Сумматоры аналоговых сигналов на ОУ. Интегрирующие и дифференцирующие схемы на ОУ. Активные фильтры на ОУ. Основные понятия алгебры логики. Способы задания логических функций. Минимизация логических функций.

Назначение и классификация сумматоров. Комбинационный сумматор на два входа. Комбинационный сумматор на три входа. Многоразрядный комбинационный сумматор.

Шифраторы. Дешифраторы. Нарастивание дешифраторов

Принцип построения мультиплексоров. Нарастивание мультиплексоров. Принцип построения демультиплексоров.

Классификация триггеров. RS – триггер на ИЛС. JK – триггер на ИЛС.

Назначение и классификация регистров. Параллельные регистры. Последовательные регистры.

Назначение и классификация счетчиков. Двоичные счетчики. Двоично-десятичные счетчики. Назначение, основные параметры запоминающих устройств (ЗУ). Структурная схема ЗУ.

Назначение и классификация микропроцессоров (МП). Основные характеристики МП. Устройство и типовые узлы МП.

Общие сведения о системе команд, форматах команд. Классификация команд. Основные команды МП.

Назначение и основные характеристики МК.

Устройство и типовые узлы микроконтроллеров.

Разработчик (и) рабочей программы:

Захаров Н.Т., преподаватель



Аннотация рабочей программы дисциплины

ОП.05 Экономика и управление

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Экономика и управление» принадлежит к циклу общепрофессиональных дисциплин..

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен уметь:

- рассчитывать по принятой методике основные технико-экономические показатели бизнес-плана;
- готовить технико-экономические предложения для организации закупок и ремонта оборудования;
- принимать управленческие решения;
- организовывать деловое общение с различными категориями работников;
- проводить инструктаж сотрудников

В результате освоения дисциплины обучающийся должен знать:

- общие положения экономической теории, маркетинга и менеджмента;
- основные элементы и технико-экономические показатели разработки бизнес-плана в области информационной безопасности;

- сущность, содержание и функции управления, порядок выработки управленческого решения и организацию его выполнения;
- формы и методы инструктажа и обучения сотрудников;
- организационное обеспечение документирования управления персоналом и трудовой деятельности работников.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 36 часа, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 36 часов, из них практическая работа – 20 часов.
- Форма контроля: 6 семестр – зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Организация в условиях рыночной экономики	<p>Понятие и виды предпринимательской деятельности. Сущность организации как основного звена экономики отраслей. Основные принципы построения экономической системы организации.</p> <p>Организационно-правовые формы хозяйствования: государственные и муниципальные унитарные предприятия. Производственный процесс на предприятии</p>
Тема 2. Производственные ресурсы предприятия	<p>Основные средства и производственные мощности предприятия.</p> <p>Оборотный капитал и оборотные средства предприятия.</p>
	<p>Практические занятия:</p> <p>Расчет производственных ресурсов предприятия по заданным параметрам.</p>
Тема 3. Основные показатели деятельности организации	<p>Издержки производства.</p> <p>Ценообразование.</p> <p>Прибыль и рентабельность предприятия.</p>
	<p>Практические занятия:</p> <p>Расчет основных показателей деятельности предприятия по заданным параметрам.</p>
Тема 4. Менеджмент: Сущность и характерные черты	<p>Менеджмент как особый вид профессиональной деятельности. Сущность и характерные черты современного менеджмента.</p> <p>Основные понятия «менеджмент», «менеджер».</p> <p>История развития менеджмента. Эволюция управленческой мысли. Этапы развития. Школы менеджмента. Менеджмент как дисциплина и наука. Особенности управляющего процесса. Объект и субъект управления.</p>

	<p>Практические занятия: Эволюция управленческой мысли. Этапы развития. Школы менеджмента. Менеджмент как дисциплина и наука.</p>
<p>Тема 5. Структура организации. Внешняя и внутренняя среда организации</p>	<p>Общая теория систем. Понятие организации с точки зрения системного подхода. Организация как основная общественная система в современных условиях. Формальная и поведенческая структура. Факторы внешней и внутренней среды организации. Основные компоненты организации с точки зрения системного подхода: цели, структура, задачи, технология, люди.</p>
	<p>Практические занятия: Понятие внешней среды организации. Факторы внешней среды организации. Факторы прямого и косвенного воздействия. Уровни воздействия на организацию факторов внешней среды.</p>
<p>Тема 6. Планирование в системе менеджмента</p>	<p>Понятие «стратегия» и «тактика», разведение понятий. Определение этапов стратегического и тактического планирования.</p>
	<p>Практические занятия: Прогнозирование. Разработка программы действия и составление графика работ Формы и стратегии планирования. Анализ внешней среды в стратегическом планировании.</p>
<p>Тема 7. Система методов управления</p>	<p>Мотивация и потребности. Деловое общение. Процесс принятия решения. Контроль и его виды.</p>
	<p>Практическое занятие: Организация контроля на предприятии.</p>
<p>Тема 8. Управление конфликтами и стрессами</p>	<p>Понятие «социальный конфликт», «организационный конфликт». Основные элементы конфликта. Этапы протекания конфликта. Виды конфликтов.</p>
<p>Тема 9. Руководство: власть и партнерство</p>	<p>Понятия «руководство» и «власть». Источники власти. Виды власти и методы влияния.</p>
	<p>Практическое занятие: Разработка системы коммуникации между руководителями и подчиненными в организации</p>

Разработчик (и) рабочей программы:
Константинова М.С., преподаватель



**Аннотация
рабочей программы дисциплины**

ОП.07 Технические средства информации

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью ППССЗ в соответствии с ФГОС СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ППССЗ

Учебная дисциплина «Технические средства информации» принадлежит к циклу общепрофессиональных дисциплин.

**3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-
ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ
ДИСЦИПЛИНЫ**

В результате освоения дисциплины обучающийся должен уметь:

— пользоваться основными видами современной вычислительной техники, периферийных и мобильных устройств и других технических средств информации;

— правильно эксплуатировать и устранять типичные выявленные дефекты технических средств информации.

В результате освоения дисциплины обучающийся должен знать:

— сущность и понятие информационной безопасности, характеристику ее составляющих;

— место информационной безопасности в системе национальной безопасности страны;

- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 118 часа, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 118 часов, из них практическая работа – 118 часов.
- Форма контроля: 4 семестр – дифференцированный зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Общая характеристика и классификация технических средств информатизации. Определение технических средств информатизации. Классификация технических средств информатизации. Устройство и принцип действия ЭВМ

Раздел 2. Основные конструктивные элементы средств вычислительной техники. Принцип работы блока питания. Виды напряжения, используемые компьютерами. Корпуса компьютеров. Общие сведения. Типы системных плат. Логическое устройство системных плат. Устройство процессора. Принцип работы. Типы процессоров. Виды оперативной памяти. Кеш память.

Раздел 3. Периферийные устройства вычислительной техники. Накопители на жестких магнитных дисках. Приводы. Мониторы. Видеоадаптеры. Звуковая система ПК. Акустическая система. Клавиатура. Оптико-механические манипуляторы. Сканеры. Принтеры. Плоттеры.

Нестандартные периферийные устройства Работа с конспектом. Изучение учебной литературы.

Раздел 4. Архитектура компьютерных систем. Арифметические основы ЭВМ. Представление информации в ЭВМ. Базовые логические операции и схемы. Таблицы истинности. Схемные логические элементы ЭВМ. Логические узлы ЭВМ и их классификация. Сумматоры, дешифраторы, их назначение и применение. Программируемые логические элементы их назначение и применение

Раздел 5. Технические средства систем дистанционной передачи информации. Структура и основные характеристики систем дистанционной передачи информации. Обмен информацией через модем. Системы сотовой подвижной связи. Спутниковые системы связи

Разработчик (и) рабочей программы:

Нерлов М.И., преподаватель



Аннотация рабочей программы дисциплины

ОП.08 Стандартизация, сертификация и техническое документоведение

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью ППССЗ в соответствии с ФГОС СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ППССЗ

Учебная дисциплина «Стандартизация, сертификация и техническое документоведение» принадлежит к циклу общепрофессиональных дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ - ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

- Применять требования нормативных актов к основным видам продукции (услуг) и процессов.
- Применять документацию систем качества.
- Применять основные правила и документы системы сертификации Российской Федерации.

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

- Правовые основы метрологии, стандартизации и сертификации.
- Основные понятия и определения метрологии, стандартизации и сертификации.

- Основные положения систем (комплексов) общетехнических и организационно-методических стандартов.
- Показатели качества и методы их оценки.
- Системы качества.
- Основные термины и определения в области сертификации.
- Организационную структуру сертификации.
- Системы и схемы сертификации.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 62 часа, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 44 часов, из них практическая работа – 22 часов.
- самостоятельная работа обучающегося (всего) 18 часов.

Форма контроля: 8 семестр – зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1 Стандартизация

Государственная система стандартизации Российской Федерации. Обеспечение качества и безопасности процессов, продукции и услуг в сфере информационных технологий, требований международных стандартов серии ИСО 9000 в части создания систем менеджмента качества, структуры и основных требований национальных и международных стандартов в сфере средств информационных технологий. Стандартизация в различных сферах. Организационная структура технического комитета ИСО 176, модель описания системы качества в стандартах ИСО 9001 и 9004 и модель функционирования системы менеджмента качества (СМК), основанной на процессном подходе. Международная стандартизация. Федеральное агентство по техническому регулированию и метрологии РФ и его основные задачи, межгосударственный совет по стандартизации, метрологии и сертификации Содружества Независимых Государств и других национальных организациях. Организация работ по стандартизации в Российской Федерации. Правовые основы стандартизации и ее задачи. Органы и службы по стандартизации. Порядок разработки стандартов. Государственный контроль и надзор за соблюдением обязательных требований стандартов. Маркировка продукции знаком соответствия государственным стандартам. Нормоконтроль технической документации. Техническое регулирование и стандартизация в области ИКТ. Обеспечение качества и безопасности процессов, продукции и услуг в сфере информационных технологий, требований международных стандартов серии

ИСО 9000 в части создания систем менеджмента качества, структуры и основных требований национальных и международных стандартов в сфере средств информационных технологий. Организация работ по стандартизации в области ИКТ и открытые системы. Федеральное агентство по техническому регулированию и метрологии РФ и его основные задачи, межгосударственный совет по стандартизации, метрологии и сертификации Содружества Независимых Государств и других национальных организациях. Стандарты и спецификации в области информационной безопасности Российское и зарубежное законодательство в области ИБ. Обзор международных национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408 и др. Системы менеджмента качества. Менеджмент качества. Предпосылки развития менеджмента качества. Принципы обеспечения качества программных средств. Основные международные стандарты в области ИТ: ISO/IEC 9126, ISO/IEC 14598 и ИСО/МЭК 9126-1.

Раздел 2 Сертификация.

Сущность и проведение сертификации. Сущность сертификации. Проведение сертификации. Правовые основы сертификации. Организационно-методические принципы сертификации. Деятельность ИСО в области сертификации. Деятельность МЭК в сертификации. Нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности. Международные правовые и нормативные акты обеспечения информационной безопасности процессов переработки информации. Отечественное организационное, правовое и нормативное обеспечения и регулирование в сфере информационной безопасности. Система менеджмента информационной безопасности. Сертификация систем обеспечения качества. Экологическая сертификация. Сертификация информационно-коммуникационных технологий и система ИНКОМТЕХСЕРТ

Раздел 3 Техническое документоведение.

Основные виды технической и технологической документации. Виды технической и технологической документации. Стандарты оформления документов, регламентов, протоколов по информационным системам.

Разработчик (и) рабочей программы:

Максимова В.В., преподаватель



Аннотация рабочей программы дисциплины

ПД.02 Информатика

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Учебная дисциплина «Информатика» принадлежит к циклу профильных дисциплин.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение содержания учебной дисциплины «Информатика» обеспечивает

достижение студентами следующих результатов:
межпредметном уровне;

– применение навыков сотрудничества со сверстниками, детьми младшего возраста, взрослыми в процессе речевого общения, образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;

– овладение нормами речевого поведения в различных ситуациях межличностного и межкультурного общения;

– готовность и способность к самостоятельной информационно- познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

– умение извлекать необходимую информацию из различных источников:

– учебно-научных текстов, справочной литературы, средств массовой информации, информационных и коммуникационных технологий для решения когнитивных, коммуникативных и организационных задач в процессе изучения информатики;

предметных:

– выполнять расчеты с использованием прикладных компьютерных программ;

– использовать сеть Интернет и ее возможности для организации оперативного обмена информацией;

– использовать технологии сбора, размещения, хранения, накопления, преобразования и передачи данных в профессионально ориентированных информационных системах;

– обрабатывать и анализировать информацию с применением программных средств и вычислительной техники;

– получать информацию в локальных и глобальных компьютерных сетях;

– применять графические редакторы для создания и редактирования изображений;

– применять компьютерные программы для поиска информации, составления и оформления документов и презентаций

В результате освоения дисциплины обучающийся должен знать:

– базовые системные программные продукты и пакеты прикладных программ;

– основные положения и принципы построения системы обработки и передачи информации;

– устройство компьютерных сетей и сетевых технологий обработки и передачи информации;

– методы и приемы обеспечения информационной безопасности;

– методы и средства сбора, обработки, хранения, передачи и накопления информации;

– общий состав и структуру персональных электронно-вычислительных машин (ЭВМ) и вычислительных систем;

– основные принципы, методы и свойства информационных и телекоммуникационных технологий, их эффективность.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальная учебная нагрузка студентов 148 часов, в том числе:

- обязательной аудиторной учебной нагрузки студентов 138 часов (в том числе практических работ 74 часов).

Форма контроля: 1 семестр – контрольная работа Форма контроля: 2 семестр – экзамен.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Информационная деятельность человека. Этапы развития информационного общества. Этапы развития технических средств и информационных ресурсов. Информационные ресурсы общества. Виды профессиональной информационной деятельности человека с использованием технических средств. Правовые нормы, относящиеся к информации.

Раздел 2. Информация и информационные процессы. Основные подходы к понятию «информация». Виды и свойства информации. Измерение информации. Кодирование информации. Системы счисления, используемые в ПК. Принципы обработки информации компьютером. Арифметические основы работы компьютера. Алгебра логики. Понятие об алгоритме, свойства, способы записи. Носитель информации: понятие, виды, основная характеристика. Способы записи информации: магнитный и оптический. Архив информации: понятие, виды, основные характеристика. Определение объёма различных носителей информации. Поиск информации, хранящейся на компьютере. Программные поисковые сервисы. Организация поиска путём использования ключевых слов и фраз. Передача информации посредством каналов связи, их основная характеристика. Характеристика организации проводной связи между компьютерами. Характеристика организации беспроводной связи между компьютерами. Электронная почта. Информационно-поисковые системы и средства работы с ними.

Раздел 3. Средства информационных и коммуникационных технологий. Архитектура ПК, характеристика основных устройств. Магистрально-модульный принцип построения компьютера. Периферийные устройства ПК: виды, основная характеристика. Примеры комплектации компьютера по профилю специальности. Программное обеспечение ПК: виды, характеристика. Понятие локальной сети. Виды, способы организации, основная характеристика ЛС. Программное обеспечение ЛС. Эксплуатационные требования к компьютерному рабочему месту. Защита информации, антивирусная защита.

Раздел 4. Технологии создания и преобразования информационных объектов. Текст как информационный объект: характерные особенности, назначение. Преобразование текста с помощью текстового редактора: редактирование, форматирование, построение таблиц, графических изображений. Структурные элементы текста, их характеристика. ЭТ как информационный объект: характерные особенности, назначение. Основные возможности ЭТ: ввод, редактирование данных. Форматы, проведение математических расчётов, использование функций, построение диаграмм и графиков. Применение ЭТ для решения профессиональных задач. Понятие БД, СУБД как информационной системы. Структурные элементы, виды БД. Этапы создания БД (разбор конкретных примеров). Основные возможности СУБД (на примере Access). Способы представления графической информации: растровая графика, векторная графика, фрактальная графика. Профессиональная графика по профилю специальности. Понятие мультимедиа. Программная реализация задач мультимедиа. Представление

графической и мультимедийной информации с помощью компьютерных презентаций (на примере P.Point).

Раздел 5. Телекоммуникационные технологии. Технические и программные средства Интернет - технологии: основные понятия, способы и скоростные характеристики подключения, ресурсы Интернет. Провайдер. Использование Интернет - технологии в профессиональной деятельности. Понятие сайта. Способы создания сайта. Основные критерии создания веб – ресурсов. Основные этапы создания сайта, их характеристика. Понятие навигации сайта. Виды навигации. Основные элементы веб – ресурса: баннер, его основная задача, технические характеристики. Другие средства для привлечения пользователей. Виды сервисных услуг глобальной сети Интернет: WWW - E-mail - Usenet - FTP – ICQ- Telnet Характерные особенности телеконференций, Интернет – телефонии. Использование тестирующих систем в учебной деятельности в локальной сети учебного заведения.

Разработчик (и) рабочей программы:

Максимова В.В., преподаватель



Аннотация рабочей программы профессионального модуля

ПМ.01. Эксплуатация автоматизированных (информационных)
систем в защищённом исполнении

10.02.05. Обеспечение информационной безопасности автоматизированных
систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Профессиональный модуль (ПМ.01) «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» принадлежит к циклу профессиональных модулей.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующие ему:

— Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

— Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

— Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

— Осуществлять проверку технического состояния, техническое

обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

— Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

— Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

— Планировать и реализовывать собственное профессиональное и личностное развитие.

— Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

— Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

— Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

— Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

— Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

— Использовать информационные технологии в профессиональной деятельности.

— Пользоваться профессиональной документацией на государственном и иностранном языках.

Иметь практический опыт:

— установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;

— администрирования автоматизированных систем в защищенном исполнении;

— эксплуатации компонентов систем защиты информации автоматизированных систем;

— диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении

Должен уметь

- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;
 - организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
 - осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;
 - производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
 - настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;
 - обеспечивать работоспособность, обнаруживать и устранять неисправности
- Должен знать:
- состав и принципы работы автоматизированных систем, операционных систем и сред;
 - принципы разработки алгоритмов программ, основных приемов программирования;
 - модели баз данных;
 - принципы построения, физические основы работы периферийных устройств;
 - теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
 - порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;
- принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Всего 1032 час, из них
на освоение МДК – 810 часов, в том числе
на промежуточную аттестацию по МДК – 6 часов,
на практики – 216 часов

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1 модуля. Установка и настройка автоматизированных (информационных) систем в защищенном исполнении	
МДК.01.01 Операционные системы	
Раздел 1. Элементы теории операционных систем. Свойства операционных систем	
Тема 1.1. Основы теории операционных систем	Содержание
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.
	Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.
	Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.
	Тематика практических занятий
	Виртуальные машины. Создание, модификация, работа
	Установка ОС
	Создание и изучение структуры разделов жесткого диска Операции с файлами
Тема 1.3. Модульная структура операционных систем, пространство пользователя	Содержание
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.
	Тематика практических занятий
	Работа в консольном и графическом режимах
Тема 1.4. Управление памятью	Содержание
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти
	Тематика практических занятий
	Мониторинг за использованием памяти
Тема 1.5. Управление процессами, многопроцессорные системы	Содержание
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие
	Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок.
	Предотвращение взаимоблокировок
	Тематика практических занятий
	Управление процессами» Наблюдение за использованием ресурсов системы

Тема 1.6. Виртуализация и облачные технологии	Содержание
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования
	Облачные технологии. Исследования в области виртуализации и облаков
	Тематика практических занятий
	Изучение примеров виртуальных машин (VMware, VBox)
Раздел 2. Безопасность операционных систем	
Тема 2.1. Принципы построения защиты информации в операционных системах	Содержание
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.
	Аутентификация, авторизация, аудит.
	Тематика практических занятий
	Управление учетными записями пользователей и доступом к ресурсам
	Аудит событий системы
	Изучение штатных средств защиты информации в операционных системах
Раздел 3. Особенности работы в современных операционных системах	
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	Содержание
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.
	Операционные системы семейства Mac OS: особенности, преимущества и недостатки.
	Архитектура Android. Приложения Android
	Тематика практических занятий
	Создание дистрибутива Linux. Установка.
	Работа в ОС Linux.
Тема 3.2. Операционная система Windows	Содержание
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.
	Тематика практических занятий
	Установка и первичная настройка Windows.
Тема 3.3. Серверные операционные системы	Содержание
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.
	Тематика практических занятий
	Работа с сетевой файловой системой.
	Работа с серверной ОС, например, AltLinux.
Примерная тематика самостоятельной работы при изучении МДК.01.01 Создание виртуальной машины. Установка операционной системы. Анализ журнала аудита ОС на рабочем месте. Изучение аналитических обзоров в области построения систем безопасности операционных систем.	

Промежуточная аттестация по МДК.01.01	
Учебная практика раздела 1 модуля	
Виды работ	
Установка программного обеспечения в соответствии с технической документацией.	
Настройка параметров работы программного обеспечения, включая системы управления базами данных.	
Настройка компонентов подсистем защиты информации операционных систем.	
Управление учетными записями пользователей.	
Работа в операционных системах с соблюдением действующих требований по защите информации.	
Установка обновления программного обеспечения.	
Контроль целостность подсистем защиты информации операционных систем.	
Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	
Использование программных средств для архивирования информации.	
Производственная практика	
Виды работ:	
Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	
Обслуживание средств защиты информации прикладного и системного программного обеспечения	
Настройка программного обеспечения с соблюдением требований по защите информации	
Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	
Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением	
Настройка встроенных средств защиты информации программного обеспечения	
Проверка функционирования встроенных средств защиты информации программного обеспечения	
Своевременное обнаружение признаков наличия вредоносного программного обеспечения	
Обслуживание средств защиты информации в компьютерных системах и сетях	
Обслуживание систем защиты информации в автоматизированных системах	
Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	
Проверка работоспособности системы защиты информации автоматизированной системы	
Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	
Контроль стабильности характеристик системы защиты информации автоматизированной системы	
Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	
Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	
МДК.01.02 Базы данных	
Раздел 1. Основы теории баз данных	
Тема 1.1. Основные понятия теории баз данных. Модели данных	<p>Содержание</p> <p>Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление</p>

	данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.
Тема 1.2. Основы реляционной алгебры	Содержание Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом. Тематика практических занятий Операции над отношениями
Тема 1.3. Базовые понятия и классификация систем управления базами данных	Содержание Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)
Тема 1.4. Целостность данных как ключевое понятие баз данных	Содержание Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.
Раздел 2. Проектирование баз данных	
Тема 2.1. Информационные модели реляционных баз данных	Содержание Типы информационных моделей. Логические модели данных. Физические модели данных. Тематика практических занятий Проектирование инфологической модели данных
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальной формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации. Тематика практических занятий Проектирование структуры базы данных
Тема 2.3. Средства автоматизации проектирования	Содержание CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования. Тематика практических занятий Проектирование базы данных с использованием CASE-средств
Раздел 3. Организация баз данных	
Тема 3.1. Создание базы данных. Манипулирование данными.	Содержание Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления,

	редактирования, удаления и восстановления данных. Навигация по набору данных.
	Тематика практических занятий
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	Содержание
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.
	Тематика практических занятий
	Создание взаимосвязей
	Сортировка, поиск и фильтрация данных
	Способы объединения таблиц
Раздел 4. Управление базой данных с помощью SQL	
Тема 4.1. Структурированный язык запросов SQL	Содержание
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.
	Тематика практических занятий
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL
Тема 4.2. Операторы и функции языка SQL	Содержание
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.
	Тематика практических занятий
	Создание и использование запросов. Группировка и агрегирование данных
	Коррелированные вложенные запросы
	Создание в запросах вычисляемых полей. Использование условий
Раздел 5. Организация распределённых баз данных	
Тема 5.1. Архитектуры распределённых баз данных	Содержание
	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределённые базы данных, параллельная обработка данных.
	Отличия и преимущества удалённых баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.
	Тематика практических занятий
	Управление доступом к объектам базы данных
Тема 5.2. Серверная часть распределённой базы данных	Содержание
	Планирование и развёртывание СУБД для работы с клиентскими приложениями
	Тематика практических занятий
	Установка СУБД. Настройка компонентов СУБД.
Тема 5.3. Клиентская	Содержание

часть распределенной базы данных	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.
	Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.
	Оптимизация производительности работы СУБД.
	Тематика практических занятий
	Создание форм и отчетов
	Создание меню. Генерация, запуск.
	Профилирование запросов клиентских приложений.
Раздел 6. Администрирование и безопасность	
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Содержание
	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.
	Тематика практических занятий
	Разработка хранимых процедур и триггеров
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	Содержание
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.
Тема 6.3. Механизмы защиты информации в системах управления базами данных	Содержание
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.
	Средства защиты информации в базах данных
	Тематика практических занятий
Тема 6.4. Копирование и перенос данных. Восстановление данных	Содержание
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных
	Тематика практических занятий
	Аудит данных с помощью средств СУБД и триггеров
Резервное копирование и восстановление баз данных	
Примерная тематика самостоятельной работы при изучении МДК.01.02	

<p>Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных».</p> <p>Выполнение индивидуального задания по теме «Нормализация отношений».</p> <p>Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД).</p> <p>Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей»</p> <p>Выполнение индивидуального задания по теме «Организация запросов».</p> <p>Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД».</p> <p>Разбор синтаксиса хранимых процедур и триггеров.</p> <p>Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».</p>	
Промежуточная аттестация по МДК.01.02	
<p>Примерные виды самостоятельных работ при изучении раздела 1 модуля</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.</p>	
Учебная практика раздела 2 модуля	
Раздел 2 модуля. Администрирование автоматизированных (информационных) систем в защищенном исполнении	
МДК.01.03 Сети и системы передачи информации	
Раздел 1. Теория телекоммуникационных сетей	
Тема 1.1. Основные понятия и определения	Содержание
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.
Тема 1.2. Принципы передачи информации в сетях и системах связи	Содержание
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.
Тема 1.3. Типовые каналы передачи и их характеристики	Содержание
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плездохронных систем передачи. Основные параметры и характеристики сигналов. Упрощенная схема организации канала ТЧ
	Тематика лабораторных работ
	Расчет пропускной способности канала связи
Раздел 2. Сети передачи данных	
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	Содержание
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.
	Протоколы и интерфейсы управления каналами и сетью передачи данных.
	Тематика лабораторных работ
	Конфигурирование сетевого интерфейса рабочей станции
	Конфигурирование сетевого интерфейса маршрутизатора по

	<p>протоколу IP</p> <p>Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне</p> <p>Диагностика и разрешение проблем сетевого уровня</p> <p>Диагностика и разрешение проблем протоколов транспортного уровня</p> <p>Диагностика и разрешение проблем протоколов прикладного уровня</p>
Тема 2.2. Беспроводные системы передачи данных	<p>Содержание</p> <p>Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX</p> <p>Тематика лабораторных работ</p> <p>Настройка Wi-Fi маршрутизатора</p>
Тема 2.3. Сотовые и спутниковые системы	<p>Содержание</p> <p>Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.</p>
<p>Примерная тематика самостоятельной работы при изучении МДК.01.03</p> <p>Настройка Wi-Fi маршрутизатора</p> <p>Изучение сетевых утилит</p> <p>Конфигурирование сетевого интерфейса</p> <p>Маршрутизация и управление потоками в сетях связи</p>	
<p>Промежуточная аттестация по МДК.01.03</p> <p>Учебная практика раздела 3 модуля</p>	
<p>МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</p>	
<p>Раздел 1. Разработка защищенных автоматизированных (информационных) систем</p>	
Тема 1.1. Основы информационных систем как объекта защиты.	<p>Содержание</p> <p>Понятие автоматизированной (информационной) системы</p> <p>Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.</p> <p>Основные особенности современных проектов АИС. Электронный документооборот.</p> <p>Тематика практических занятий и лабораторных работ</p> <p>Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)</p>
Тема 1.2. Жизненный цикл автоматизированных систем	<p>Содержание</p> <p>Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.</p>

	Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.
	Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.
	Тематика практических занятий и лабораторных работ
	Разработка технического задания на проектирование автоматизированной системы
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	Содержание
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации
	Понятие уязвимости угрозы. Классификация уязвимостей.
	Тематика практических занятий и лабораторных работ
	Категорирование информационных ресурсов
	Анализ угроз безопасности информации
	Построение модели угроз
Тема 1.4. Основные меры защиты информации в автоматизированных системах	Содержание
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание
	Идентификация и аутентификация субъектов доступа и объектов доступа.
	Управление доступом субъектов доступа к объектам доступа.
	Ограничение программной среды.
	Защита машинных носителей информации
	Регистрация событий безопасности
	Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.
	Обнаружение (предотвращение) вторжений
	Тематика практических занятий и лабораторных работ
	Контроль (анализ) защищенности информации
	Обеспечение целостности информационной системы и информации
	Обеспечение доступности информации
Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	
Защита технических средств.	
Защита информационной системы, ее средств, систем связи и передачи данных	

	Резервное копирование и восстановление данных.
	Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
Тема 1.6. Защита информации в распределенных автоматизированных системах	Содержание Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.
Тема 1.7. Особенности разработки информационных систем персональных данных	Содержание Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности. Тематика практических занятий и лабораторных работ Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.
Раздел 2. Эксплуатация защищенных автоматизированных систем.	
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении
Тема 2.2. Администрирование автоматизированных систем	Содержание Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.
Тема 2.4. Защита от несанкционированного доступа к информации	Содержание Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД. Классификация автоматизированных систем. Требования по

	защите информации от НСД для АС
	Требования защищенности СВТ от НСД к информации
	Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ
Тема 2.5. СЗИ от НСД	Содержание
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.
	Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.
	Обеспечение целостности информационной системы и информации
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности
	Тематика практических занятий и лабораторных работ
	Установка и настройка СЗИ от НСД
	Защита входа в систему (идентификация и аутентификация пользователей)
	Разграничение доступа к устройствам
	Управление доступом
	Использование принтеров для печати конфиденциальных документов. Контроль печати
	Настройка системы для задач аудита
	Настройка контроля целостности и замкнутой программной среды
	Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности
	Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях
Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	
Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	
Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	
Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	
Тематика практических занятий и лабораторных работ	
Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных	

	систем
Тема 2.7. Документация на защищаемую автоматизированную систему	Содержание
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.
	Тематика практических занятий и лабораторных работ
	Оформление основных эксплуатационных документов на автоматизированную систему.
Примерная тематика самостоятельной работы при изучении МДК.01.04	
1. Разработка концепции защиты автоматизированной (информационной) системы	
2. Анализ банка данных угроз безопасности информации	
3. Анализ журнала аудита ОС на рабочем месте	
4. Построение сводной матрицы угроз автоматизированной (информационной) системы	
5. Анализ политик безопасности информационного объекта	
6. Изучение аналитических обзоров в области построения систем безопасности	
7. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации	
Промежуточная аттестация по МДК.01.04	
Учебная практика раздела 4 модуля	
МДК.01.05. Эксплуатация компьютерных сетей	
Раздел 1. Основы передачи данных в компьютерных сетях	
Тема 1.1. Модели сетевого взаимодействия	Содержание
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.
	Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.
	Тематика лабораторных работ
	Изучение элементов кабельной системы.
Тема 1.2. Физический уровень модели OSI	Содержание
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.
	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.
	Оптоволоконные линии связи
	Стандарты кабелей. Электрическая проводка.
	Беспроводная среда передачи.
	Тематика лабораторных работ
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)
	Сварка оптического волокна
Тема 1.3. Топология компьютерных сетей	Содержание
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.
	Тематика лабораторных работ
	Разработка топологии сети небольшого предприятия

	Построение одноранговой сети
Тема 1.4. Технологии Ethernet	Содержание
	Обзор технологий построения локальных сетей.
	Технология Ethernet. Физический уровень.
	Технология Ethernet. Канальный уровень
	Тематика лабораторных работ
	Изучение адресации канального уровня. MAC-адреса.
Тема 1.5. Технологии коммутации	Содержание
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.
	Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети
	Технология PoweroverEthernet
	Тематика лабораторных работ
	Создание коммутируемой сети
Тема 1.6. Сетевой протокол IPv4	Содержание
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.
	Маршрутизация пакетов IPv4
	Протоколы динамической маршрутизации
	Тематика лабораторных работ
	Изучение IP-адресации.
Тема 1.7. Скоростные и беспроводные сети	Содержание
	Сеть FDDI. Сеть 100VG-AnyLAN
	Сверхвысокоскоростные сети
	Беспроводные сети
	Тематика лабораторных работ
	Настройка беспроводного сетевого оборудования
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet	
Тема 2.1. Основы коммутации	Содержание
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов.
	Управление потоком в полудуплексном и дуплексном режимах.
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов
	Тематика лабораторных работ
	Работа с основными командами коммутатора.
Тема 2.2. Начальная настройка коммутатора	Содержание
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.
	Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.
	Тематика лабораторных работ
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов

	Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы
Тема 2.3. Виртуальные локальные сети (VLAN)	Содержание
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.
	Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation
	Тематика лабораторных работ
	Настройка VLAN на основе стандарта IEEE 802.1Q
	Настройка протокола GVRP.
	Настройка сегментации трафика без использования VLAN
	Настройка функции Q-in-Q (Double VLAN).
	Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.
Тема 2.4. Функции повышения надежности и производительности	Содержание
	Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.
	Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.
	Дополнительные функции защиты от петель. Агрегирование каналов связи.
	Тематика лабораторных работ
	Настройка протоколов связующего дерева STP, RSTP, MSTP.
	Настройка функции защиты от образования петель LoopBackDetection
Агрегирование каналов.	
Тема 2.5. Адресация сетевого уровня и маршрутизация	Содержание
	Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.
	Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.
	Планирование подсетей IPv6. Протокол NDP.
	Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.
	Тематика лабораторных работ
	Основные конфигурации маршрутизатора.
	Расширенные конфигурации маршрутизатора.
	Работа с протоколом CDP.
	Работа с протоколом TELNET. Работа с протоколом TFTP.
	Работа с протоколом RIP.
	Работа с протоколом OSPF.
	Конфигурирование функции маршрутизатора NAT/PAT.
Конфигурирование PPP и CHAP.	
Тема 2.6. Качество обслуживания (QoS)	Содержание
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.

	Тематика лабораторных работ
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	Содержание
	Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.
	Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.
	Тематика лабораторных работ
	Списки управления доступом (AccessControlList)
	Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.
	Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding
Тема 2.8. Многоадресная рассылка	Содержание
	Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.
	Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping). Функция IGMP FastLeave.
	Тематика лабораторных работ
	Отслеживание трафика многоадресной рассылки.
	Отслеживание трафика Multicast
Тема 2.9. Функции управления коммутаторами	Содержание
	Управление множеством коммутаторов. Протокол SNMP.
	RMON (Remote Monitoring). Функция Port Mirroring.
	Тематика лабораторных работ
	Функции анализа сетевого трафика.
	Настройка протокола управления топологией сети LLDP.
Раздел 3. Межсетевые экраны	
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Содержание
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.
Тема 3.2. Межсетевые экраны	Содержание
	Технологии межсетевых экранов. Политика меж сетевого экрана. Межсетевые экраны с возможностями NAT.
	Топология сети при использовании межсетевых экранов. Планирование и внедрение меж сетевого экрана.
	Тематика лабораторных работ
	Основы администрирования меж сетевого экрана
	Соединение двух локальных сетей межсетевыми экранами
	Создание политики без проверки состояния.
	Создание политик для традиционного (или исходящего) NAT.
	Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing
Тема 3.3. Системы обнаружения и	Содержание
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.

предотвращения проникновений	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.
	Тематика лабораторных работ
	Обнаружение и предотвращение вторжений.
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Содержание
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.
	Тематика лабораторных работ
	Создание альтернативных маршрутов с использованием статической маршрутизации
<p>Примерная тематика самостоятельной работы при изучении МДК.01.05</p> <p>Физическое кодирование с использованием манчестерского кода</p> <p>Логическое кодирование с использованием скремблирования</p> <p>Подключение клиента к беспроводной сети в инфраструктурном режиме</p> <p>Оценка беспроводной линии связи</p> <p>Проектирования беспроводной сети</p> <p>Сбор информации о клиентских устройствах</p> <p>Планирование производительности и зоны действия беспроводной сети</p> <p>Предпроектное обследование места установки беспроводной сети</p> <p>Обеспечение отказоустойчивости в беспроводных сетях</p> <p>Режимы работы и организация питания точек доступа</p> <p>Сегментация беспроводной сети</p> <p>Настройка QoS</p> <p>Постпроектное обследование и тестирование сети</p> <p>Создание ACL-списка</p> <p>Наблюдение за трафиком в сети VLAN</p> <p>Определение уязвимых мест сети</p> <p>Реализация функций обеспечения безопасности порта коммутатора</p> <p>Исследование трафика</p> <p>Создание структуры сети организации</p> <p>Определение технических требований</p> <p>Мониторинг производительности сети</p> <p>Создание диаграммы логической сети</p> <p>Подготовка к обследованию объекта</p> <p>Обследование зоны беспроводной связи</p> <p>Формулировка общих целей проекта</p> <p>Разработка требований к сети</p> <p>Анализ существующей сети</p> <p>Определение характеристик сетевых приложений</p> <p>Анализ сетевого трафика</p> <p>Определение приоритетности трафика</p> <p>Изучение качества обслуживания сети</p> <p>Исследование влияния видеотрафика на сеть</p> <p>Определение потоков трафика, построение диаграмм потоков трафика</p> <p>Применение проектных ограничений</p> <p>Определение проектных стратегий для достижения масштабируемости</p> <p>Определение стратегий повышения доступности</p> <p>Определение требований к обеспечению безопасности</p> <p>Разработка ACL-списков для реализации наборов правил межсетевого экрана</p> <p>Использование CIDR для обеспечения объединения маршрутов</p> <p>Определение схемы IP-адресации</p>	

<p>Определение количества IP-сетей Создание таблицы для выделения адресов Составление схемы сети Анализ плана тестирования и выполнение теста Создание плана тестирования для сети комплекса зданий Проектирование виртуальных частных сетей Безопасная передача данных в беспроводных сетях</p>
<p>Промежуточная аттестация по МДК.01.05</p>
<p>Учебная практика раздела 5 модуля</p>
<p>Примерные виды самостоятельных работ при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.</p>
<p>Экзамен по профессиональному модулю (демонстрационный экзамен)</p>

Разработчик (и) рабочей программы:
Крымова О.В., преподаватель



Аннотация рабочей программы профессионального модуля

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Профессиональный модуль (ПМ.02) «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» принадлежит к циклу профессиональных модулей.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ- ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения профессионального модуля студент должен:

Иметь практический опыт:

- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;
- учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;
- работы с подсистемами регистрации событий;
- выявления событий и инцидентов безопасности в автоматизированной системе.

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.

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.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося 720 часов, в том числе:

- обязательная аудиторная учебная нагрузка (всего) 452 часов;
- лабораторная работа 262 часов

- самостоятельная работа 82 часов.
- Форма контроля:
- 6 семестр – экзамен;
- 6 семестр – дифференцированный зачет;
- 6 семестр – курсовая работа.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Основные разделы профессионального модуля..

МДК.02.01. Программные и программно-аппаратные средства защиты информации.

Тема 1. Предмет и задачи программно-аппаратной защиты информации

Тема 2. Стандарты безопасности

Тема 3. Защищенная автоматизированная система

Тема 4. Дестабилизирующее воздействие на объекты защиты

Тема 5. Принципы программно-аппаратной защиты информации от несанкционированного доступа организации

МДК.02.02. Криптографические средства защиты информации

Тема 1. Математические основы криптографии

Тема 2. Методы криптографической защиты информации

Тема 3. Криптоанализ

Тема 4. Поточные шифры и генераторы псевдослучайных чисел

Тема 5. Кодирование информации.

Компьютеризация шифрования.

Тема 6. Симметричные системы шифрования

Тема 7. Асимметричные системы шифрования

Тема 8. Аутентификация данных. Электронная подпись

Тема 9. Алгоритмы обмена ключей и протоколы аутентификации

Тема 10. Криптозащита информации в сетях передачи данных

Тема 11. Защита информации в электронных платежных системах

Тема 12. Компьютерная стеганография

Разработчик (и) рабочей программы:

Михайлов И.И., преподаватель



Аннотация рабочей программы профессионального модуля

ПМ.03. Защита информации техническими средствами

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Профессиональный модуль (ПМ.03) «Защита информации техническими средствами» принадлежит к циклу профессиональных модулей.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;

- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

- проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

- установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

В результате освоения профессионального модуля обучающийся должен уметь:

- применять технические средства для криптографической защиты информации конфиденциального характера;

- применять технические средства для уничтожения информации и носителей информации;

- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

- применять инженерно-технические средства физической защиты объектов информатизации

В результате освоения профессионального модуля обучающийся

должен знать:

- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Максимальной учебной нагрузки обучающегося – 564 часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – 382 часов;

самостоятельной работы обучающегося – 68 часов;
 учебной практики – 36 часа;
 производственной практики – 180 часов.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1 модуля. Применение технической защиты информации	
МДК.03.01 Техническая защита информации	
Раздел 1. Концепция инженерно-технической защиты информации	
Тема 1.1. Предмет и задачи технической защиты информации	Содержание
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации.
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации..
Раздел 2. Теоретические основы инженерно-технической защиты информации	
Тема 2.1. Информация как предмет защиты	Содержание
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
	Тематика практических занятий и лабораторных работ
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. Организация аттестации защищаемого помещения по требованиям безопасности информации.
Тема 2.2. Технические каналы утечки информации	Содержание
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки

	информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
	Тематика практических занятий и лабораторных работ
	Индикаторы электромагнитного поля Сканирующие радиоприемники Анализаторы спектра, радиочастотомеры Многофункциональные комплекты для выявления каналов утечки информации Комплекс RS turbo
Тема 2.3. Методы и средства технической разведки	Содержание
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.
	Тематика практических занятий и лабораторных работ
	Комплексы измерения ПЭМИН Нелинейные локаторы Комплекс для измерения характеристик акустических сигналов «Спрут-7» Металлодетекторы Портативная рентгенотелевизионная установка «Норка» Досмотровые эндоскопы
Раздел 3. Физические основы технической защиты информации	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей
	Тематика практических занятий и лабораторных работ
	Исследование акустического и виброакустического каналов утечки информации с помощью универсального поискового прибора ST 033P «Пиранья». Поиск технических средств негласного получения информации с помощью универсального поискового прибора ST 033P «Пиранья»
Тема 3.2.	Содержание

Физические процессы при подавлении опасных сигналов	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.
	Тематика практических занятий и лабораторных работ
	Проверка выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью комплекса «Спрут-мини».
Раздел 4. Системы защиты от утечки информации	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
	Тематика практических занятий и лабораторных работ
	Защита от утечки по акустическому каналу
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.
	Тематика практических занятий и лабораторных работ
	Изучение портативных диктофонов
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.
	Тематика практических занятий и лабораторных работ
	Защита от утечки по виброакустическому каналу
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты

	информации от несанкционированной утечки по электромагнитному каналу.
	Тематика практических занятий и лабораторных работ
	Определение каналов утечки ПЭМИН
	Защита от утечки по цепям электропитания и заземления
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
	Тематика практических занятий и лабораторных работ
	Методы и средства защиты информации от несанкционированной утечки по телефонному каналу.
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
	Тематика практических занятий и лабораторных работ
	Проверка выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу с помощью комплекса «Спрут-мини».
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.
	Тематика практических занятий и лабораторных работ
	Проверка выполнения норм эффективности защиты речевой информации от утечки за счет электроакустических преобразований в ТСПИ с помощью комплекса «спрут-мини»
Раздел 5. Применение и эксплуатация технических средств защиты информации	
Тема 5.1. Применение технических средств защиты информации	Содержание
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими

	<p>средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</p> <p>Тематика практических занятий и лабораторных работ</p> <p>Проведение измерений акустоэлектрического эффекта с использованием нановольтметра Unipan 233.</p>
Тема 5.2.	Содержание
Эксплуатация технических средств защиты информации	<p>Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.</p> <p>Тематика практических занятий и лабораторных работ</p> <p>Оценка защищенности информации от утечки по каналу ПЭМИ с использованием селективных микровольтметров SMV 8.5 и SMV 11 в диапазоне частот 9кГц-1ГГц.</p>
	Тематика практических занятий и лабораторных работ
	Оценка защищенности информации от утечки по каналу ПЭМИ с использованием селективных микровольтметров SMV 8.5 и SMV 11 в диапазоне частот 9кГц-1ГГц.
<p>Примерная тематика самостоятельной работы при изучении МДК.03.01</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.</p>	
<p>Учебная практика</p> <p>Виды работ:</p> <p>Измерение параметров физических полей.</p> <p>Определение каналов утечки ПЭМИН.</p> <p>Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</p> <p>Установка и настройка технических средств защиты информации.</p> <p>Проведение измерений параметров побочных электромагнитных излучений и наводок.</p> <p>Проведение аттестации объектов информатизации.</p>	
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	
МДК.03.02	Инженерно-технические средства физической защиты объектов информатизации
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты	

Тема 1.1. Цели и задачи физической защиты объектов информатизации	<p>Содержание</p> <p>Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.</p>
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	<p>Содержание</p> <p>Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.</p> <p>Тематика практических занятий и лабораторных работ</p> <p>Изучение основных нормативных документов в области систем видеонаблюдения Разработка и утверждение технического задания. Работа с прайс-листами. Проектирование системы видеонаблюдения. Изучение особенностей выбора и расположения компонентов систем видеонаблюдения. Монтаж системы видеонаблюдения: установка аналоговых или IP-видеокамер, видеорегистраторов, монтаж электропроводок, установка источников резервного питания. Расчет емкости накопителей памяти. Настройка программного обеспечения. Отладка системы видеонаблюдения.</p>
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты	
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	<p>Содержание</p> <p>Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.</p>
Тема 2.2. Система контроля и управления доступом	<p>Содержание</p> <p>Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование</p>

	и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.
Тема 2.3. Система телевизионного наблюдения	Содержание
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.
Тема 2.5 Система воздействия	Содержание
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.
	Тематика практических занятий и лабораторных работ
	Проектирование и монтаж системы пожарной и охранной сигнализации. Изучение требований к электроснабжению технических средств охранной, пожарной и охранно-пожарной сигнализации. Изучение общих требований к монтажу ОПС. Изучение источников питания ТС ОПС. Заземление и зануление технических средств сигнализации. Монтаж охранных извещателей. Монтаж пожарных извещателей. Монтаж Приемно-контрольных приборов. Монтаж тревожной сигнализации. Монтаж периметральных технических средств сигнализации. Монтаж электропроводки объектовых технических средств сигнализации. Монтаж электропроводки линейной части сигнализации. Изучение требований к монтажу технических средств сигнализации в пожароопасных зонах. Изучение требований к монтажу технических средств сигнализации во взрывоопасных зонах. Пусконаладочные работы при монтаже установок охранной, пожарной и охранно-пожарной сигнализации.
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты	
Тема 3.1 Применение инженерно-технических	Содержание
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на

средств физической защиты	КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.
Тема	3.2. Содержание
Эксплуатация инженерно-технических средств физической защиты	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты. Организация ремонта технических средств физической защиты.
	Тематика практических занятий и лабораторных работ
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Рассмотрение принципов устройства, работы и применения средств контроля доступа. Изучение организации пропускного режима на предприятии. Разработка инструкции о пропускном режиме. Выбор СКУД для оборудования объекта. Проектирование СКУД. Монтаж электропроводок технических средств СКУД на объекте. Проведение пуско-наладочных работ.
Курсовой проект (работа)	
<p>Примерная тематика курсового проекта (работы)</p> <p>Расчет основных показателей качества системы охранной сигнализации объекта информатизации.</p> <p>Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.</p> <p>Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.</p>	
<p>Примерная тематика самостоятельной работы при изучении МДК.03.02</p> <p>Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.</p> <p>Размещение периметровых средств обнаружения на местности.</p> <p>Самостоятельное изучение порядка допуска субъектов на охраняемые объекты.</p>	
Промежуточная аттестация по МДК.03.02	
<p>Примерные виды самостоятельной работы при изучении раздела 2 модуля</p> <p>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)</p> <p>Подготовка к практическим работам с использованием методических рекомендаций</p>	

<p>преподавателя, оформление лабораторно-практических работ, отчетов к их защите.</p> <p>Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.</p>
<p>Учебная практика по разделу 2 модуля</p> <p>Монтаж различных типов датчиков.</p> <p>Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.</p> <p>Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.</p> <p>Рассмотрение системы контроля и управления доступом.</p> <p>Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.</p> <p>Рассмотрение датчиков периметра, их принципов работы.</p> <p>Выполнение звукоизоляции помещений системы зашумления.</p> <p>Реализация защиты от утечки по цепям электропитания и заземления.</p> <p>Разработка организационных и технических мероприятий по заданию преподавателя;</p> <p>Разработка основной документации по инженерно-технической защите информации.</p>
<p>Производственная практика профессионального модуля</p> <p>Виды работ</p> <p>Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;</p> <p>Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;</p> <p>Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съема и утечки по техническим каналам;</p> <p>Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.</p>
<p>Экзамен по профессиональному модулю</p>

Разработчик (и) рабочей программы:
Крымова О.В., преподаватель



Аннотация рабочей программы профессионального модуля

**ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ:14995 НАЛАДЧИК
ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ**

10.02.05. Обеспечение информационной безопасности автоматизированных систем

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ СПССЗ

Профессиональный модуль (ПМ.04) «ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ:14995 НАЛАДЧИК ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ» принадлежит к циклу профессиональных модулей.

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ-ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Иметь практический опыт	<ul style="list-style-type: none">— выполнения работ по подключению к глобальным компьютерным сетям;— установки и настройки сетевого и серверного оборудования для подключения к глобальным сетям (Интернет);— установки и настройки программного обеспечения для работы с ресурсами и сервисами установки и настройки программного обеспечения для работы с ресурсами и сервисами Интернет;— диагностики и мониторинга параметров сетевых подключений, устранения простейших неисправностей и сбоев в работе;
уметь	<ul style="list-style-type: none">— устанавливать и настраивать подключения к сети Интернет с помощью различных технологий и специализированного оборудования;— осуществлять выбор технологии подключения и тарифного плана у провайдера доступа к сети Интернет;— устанавливать специализированные программы и драйверы, осуществлять настройку параметров подключения к сети Интернет;— осуществлять диагностику подключения к сети Интернет;

	<ul style="list-style-type: none"> — осуществлять управление и учет входящего и исходящего трафика сети; — интегрировать локальную компьютерную сеть в сеть Интернет; — устанавливать и настраивать программное обеспечение серверов сети Интернет, в том числе web-серверов и серверов электронной почты; — вести отчетную и техническую документацию;
знать	<ul style="list-style-type: none"> — систему имен, адресации и маршрутизации трафика в сети Интернет; — требования к аппаратному обеспечению персональных компьютеров, серверов и периферийных устройств подключения к сети Интернет, а так же назначение и конфигурацию программного обеспечения; — виды технологий и специализированного оборудования для подключения к сети Интернет; — сведения о структуре и информационных ресурсах сети Интернет; — функции и обязанности Интернет провайдеров; — принципы функционирования, организации и структуру web-сайтов; — принципы работы с каталогами и информационно-поисковыми системами в сети Интернет.

4. КОЛИЧЕСТВО ЧАСОВ НА ОСВОЕНИЕ ПРОГРАММЫ ДИСЦИПЛИНЫ

Всего 294 час, из них
на освоение МДК – 144 часа, в том числе
на промежуточную аттестацию по МДК – 6 часов,
на практики – 144 часов

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел ПМ 1. «Охрана труда и техника безопасности»	
МДК.02.01. Установка и настройка аппаратных и программных средств доступа в сеть Интернет	
Тема 1.1. Режим труда и отдыха при работе на ПЭВМ. Требования безопасности при работе на ПЭВМ.	УЕ 1-01. «Режим труда и отдыха при работе на ПЭВМ. Требования безопасности при работе на ПЭВМ.»
Раздел 2: «Компьютерные сети»	
МДК.02.01. Установка и настройка аппаратных и программных средств доступа в сеть Интернет	
Тема 2.1. Понятие сети. Классификация сетей. Классификация локальной сети: одноранговые сети, иерархические сети. Достоинства и недостатки.	УЕ 2-01. Понятие сети. Классификация локальной сети: одноранговые сети, иерархические сети. Достоинства и недостатки.

Тема 2.2. Топология сетей.	УЕ 2-02. Топология сетей
Тема 2.3. Аппаратное обеспечение сетей.	УЕ 2-03. Аппаратное обеспечение сетей Практическая работа № 1. Аппаратное обеспечение компьютерных сетей. Подключение и настройка.
Тема 2.4. Программное обеспечение сетей	УЕ 2-04. Программное обеспечение сетей. Практическая работа № 2. Программное обеспечение компьютерных сетей. Установка и отладка.
Раздел 3: «Глобальные компьютерные сети. Интернет»	
МДК.02.01. Установка и настройка аппаратных и программных средств доступа в сеть Интернет	
Тема 3.1. Глобальная компьютерная сеть Интернет. IP-адрес, доменная система имен.	УЕ 3-01. Глобальная компьютерная сеть Интернет. IP-адрес, доменная система имен. Практическая работа № 3. Определение и запись IP-адреса.
Тема 3.2. Протокол передачи данных TCP/IP и транспортный протокол TCP.	УЕ 3-02. Протокол передачи данных TCP/IP и транспортный протокол TCP. Практическая работа № 4 Протокол передачи данных TCP/IP и транспортный протокол TCP. Настройка сетевых протоколов.
Раздел 4: «Технология подключения к сети Интернет»	
МДК.02.01. Установка и настройка аппаратных и программных средств доступа в сеть Интернет	
Тема 4.1. Виды доступа в Интернет.	УЕ 4-01. Виды доступа в Интернет
Тема 4.2. Коммутируемый удаленный доступ.	УЕ 4-02. Коммутируемый удаленный доступ
Тема 4.3. Проводная технология Ethernet – выделенные линии доступа к сети Интернет	УЕ 4-03. Проводная технология Ethernet – выделенные линии доступа к сети Интернет Практическая работа № 5 Подключение к сети Интернет по выделенной линии доступа.
Тема 4.4. Технология XDSL – цифровая абонентская линия.	УЕ 4-04. Технология XDSL – цифровая абонентская линия. Практическая работа № 6 Подключение к сети Интернет по цифровой абонентской линии.
Тема 4.5. Беспроводные технологии доступа к сети Интернет. Wi-Fi.	УЕ 4-05. Беспроводные технологии доступа к сети Интернет. Wi-Fi. Практическая работа № 7 Подключение к сети Интернет через Wi-Fi.
Тема 4.6. Доступ в Интернет через спутник.	УЕ 4-06. Доступ в Интернет через спутник Практическая работа № 8 Подключение к сети Интернет через спутник.
Тема 4.7. Доступ в Интернет через мобильный телефон.	УЕ 4-07. Доступ в Интернет через мобильный телефон Практическая работа № 9 Подключение к сети Интернет через мобильный телефон.
Тема 4.8. Трафик. Контроль трафика	Практическая работа № 10 Контроль трафика

Раздел 5: «Информационные ресурсы и службы сети Интернет»	
МДК.02.01. Установка и настройка аппаратных и программных средств доступа в сеть Интернет	
Тема 5.1. Всемирная паутина. Технология WWW. Браузеры.	УЕ 5-01. Всемирная паутина. Технология WWW. Браузеры.
	Практическая работа № 11 Изучение работы системы доменных имен (DNS), «Всемирной паутины» (WWW), браузеров и веб-серверов.
Тема 5.2. Электронная почта и телеконференции.	УЕ 5-02. Электронная почта и телеконференции.
	Практическая работа № 12 Изучение работы электронной почты. Регистрация ящика. Переписка.
	Практическая работа № 13 Организация телеконференции.
Тема 5.3. Поиск информации в Интернете. Поисковые системы общего назначения. Систематизированные поисковые системы.	УЕ 5-03. Поиск информации в Интернете. Поисковые системы общего назначения. Систематизированные поисковые системы.
	Практическая работа № 14 Знакомство с интерфейсом поисковых систем. Изучение их достоинств и недостатков.
	Практическая работа № 15 Работа с сетевыми сервисами: списки рассылки, группы новостей и другими сервисами Интернета: трехмерная карта планеты. Поиск информации в Интернете. Сохранение результатов поиска.
	Практическая работа № 16 Основы общения в Интернете. Интерактивное общение в интернете.
Тема 5.4. Файловые архивы.	УЕ 5-04. Файловые архивы.
	Практическая работа № 15 Создание, изучение и работа с файловыми архивами.