МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯРОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждениевысшего образования
«Дагестанский государственный университет»

Колледж

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01. ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

по программе подготовки специалистов среднего звена (ППССЗ)
среднего профессионального образования

Специальность:	*10.02.05 Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*среднее общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала – 2021

Рабочая программа профессионального модуля «ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении» разработана на основе ФГОС СПО по специальности по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем от 9 декабря 2016 г. № 1553 утвержденного приказом Министерства образованияи науки с учетом примерной основной образовательной программы.

Организация-разработчик: Колледж федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет»

Автор-разработчик:
Шамсутдинова У.А. - преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ДГУ
Шахбанова З.И. – преподаватель кафедры общепрофессиональных дисциплин Колледжа ДГУ
Шахбанова М.И. - преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ДГУ ВО «Дагестанский государственный университет»

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол № 7 от «27» 02 2021г.

Зав. кафедрой _____ /Магомедова А.М./

Рабочая программа профессионального модуля согласована с учебно-методическим управлением
«16» 03 2021 г. _____
(подпись)

Программа профессионального модуля согласована с представителем работодателя
Нач. отдела информационной безопасности Минпромторга РД
(полное наименование организации и должности руководителя)
Меджидов Артур Гаирович
ФИО
(подпись)
М.П.

СОДЕРЖАНИЕ

1. **ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
2. **СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
3. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Профессиональный модуль «Эксплуатация автоматизированных систем в защищенном исполнении» относится к профессиональному циклу ПССЗ.

1.3. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности: иметь практический опыт по осуществлению полномочий оператора электронно-вычислительных и вычислительных машин и соответствующие ему общие компетенции и профессиональные компетенции:

Общие компетенции

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты
автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями
эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность
автоматизированных (информационных) систем в защищенном исполнении.

В результате освоения профессионального модуля студент должен:

Иметь практическийопыт:

– 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.

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 устранятьнеисправности

Знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ,основных приемов программирования;

– модели баз данных;

– принципыпостроения, физические основы работы периферийныхустройств;

– 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.

Количество часов, отводимое на освоение профессионального модуля
Всего часов 876 часа,
из них: освоение МДК 732 часов,
Производственная практика 144 часа.

1. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Код профессиональных компетенций	**Наименование разделов профессионального модуля**	**Всего,** часов	**Объем времени, отведенный на освоение междисциплинарного курса(курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузкаобучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов
			Всего, часов	**В т.ч. лабораторные работы и практические занятия,** часов (в т.ч. практическая подготовка)	**В т.ч. курсовая работа (проект),** часов	**Всего,** часов	**В т.ч. курсовая работа (проект),** часов		
1	2	3	4	5	6	7	8	9	10
ПК1.2 ПК1.3	**МДК.01.01 Эксплуатация автоматизированных систем в защищенном исполнении**	364	364	178		63			
ПК1.2 ПК1.3 ПК1.4	**МДК.01.02 Эксплуатация компьютерных сетей**	112	112	60		20			
ПК1.1 ПК1.2	**МДК.01.03 Сети и системы передачи информации**	144	144	60		23			
ПК1.1 ПК1.2 ПК1.3	**МДК.01.04 Антивирусные системы**	112	112	60		20			
ПК1.1 ПК1.2 ПК1.3 ПК1.4	**ПП.01.01 Производственная практика, (по профилю специальности),** часов	144							144
Всего:		**876**	**732**	**358**		**126**			**144**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работаобучающихся	Объем часов
1	2	3
МДК.01.01 Эксплуатация автоматизированных систем в защищенном исполнении		**364**
Раздел 1. Разработка защищенных автоматизированных (информационных) систем		**112**
Тема 1.1. Основы информационных систем как объекта защиты.	***Лекции***	***10***
	Лекция 1.1.1. Понятие автоматизированной (информационной) системы 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	6
	Лекция 1.1.2. Основные особенности современных проектов АИС. Электронный документооборот.	4
	Практические занятия	***8***
	Практическое занятие 1.1.1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	8
Тема 1.2. Жизненный цикл автоматизированных систем	***Лекции***	***8***
	Лекция 1.2.1. 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.	4
	Лекция 1.2.2. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2
	Лекция 1.2.3. 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.	2
	Практические занятия	***4***
	Практическое занятие 1.2.1. Разработка технического задания на проектирование автоматизированной системы	4
	Самостоятельная работа обучающихся	***2***

	1.2.1. Разработка концепции защиты автоматизированной (информационной) системы	2
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	***Лекции***	***4***
	Лекция 1.3.1. 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	2
	Лекция 1.3.2. Понятие уязвимости угрозы. Классификация уязвимостей.	2
	Практические занятия	***10***
	Практическое занятие 1.3.1. Категорирование информационных ресурсов	2
	Практическое занятие 1.3.2. Анализ угроз безопасности информации	4
	Практическое занятие 1.3.3. Построение модели угроз	4
	Самостоятельная работа обучающихся	***2***
	1.3.1. Анализ банка данных угроз безопасности информации	2
Тема 1.4. Основные меры защиты информации в автоматизированных системах	***Лекции***	***4***
	Лекция 1.4.1. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	2
	Лекция 1.4.2. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	***Лекции***	***28***
	Лекция 1.5.1. Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	4
	Лекция 1.5.2. Ограничение программной среды. Защита машинных носителей информации	2
	Лекция 1.5.3. Регистрация событий безопасности	2
	Лекция 1.5.4. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	4
	Лекция 1.5.5. Обнаружение (предотвращение) вторжений	2
	Лекция 1.5.6. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.	4
	Лекция 1.5.7. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	2
	Лекция 1.5.8. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.	2
	Лекция 1.5.9. Резервное копирование и восстановление данных.	2
	Лекция 1.5.10. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	4
Тема 1.6. Защита	***Лекции***	***2***

информации в распределенных автоматизированных системах	Лекция 1.6.1. 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.	2
Тема 1.7. Особенности разработки информационных систем персональных данных	***Лекции***	10
	Лекция 1.7.1. 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.	10
	Практические занятия	6
	Практическое занятие 1.7.1. Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	6
Раздел 2. Эксплуатация защищенных автоматизированных систем.		***136***
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	***Лекции***	***62***
	Лекция 2.1.1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	26
	Лекция 2.1.2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	24
	Лекция 2.1.3. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	12
	Самостоятельная работа обучающихся	***48***
	2.1.1. Анализ журнала аудита ОС на рабочем месте	16
	2.1.2. Построение сводной матрицы угроз автоматизированной (информационной) системы	16
	2.1.3. Анализ политик безопасности информационного объекта	16
Тема 2.2. Администрирование автоматизированных систем	***Лекции***	***28***
	Лекция 2.2.1. 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.	28
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	***Лекции***	***28***
	Лекция 2.3.1. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	28
	Промежуточная аттестация в форме дифференцированного зачета	
	Курсовая работа	

Раздел 3. Защита от несанкционированного доступа к информации в автоматизированных системах		***116***
Тема 3.1. Защита от несанкционированного доступа к информации	***Лекции***	***16***
	Лекция 3.1.1. 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.	4
	Лекция 3.1.2. Классификация автоматизированных систем. Требования по защите информации от НСД для АС	4
	Лекция 3.1.3 Требования защищенности СВТ от НСД к информации	4
	Лекция 3.1.4. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	4
	Самостоятельная работа обучающихся	***4***
	3.1.5. Изучение аналитических обзоров в области построения систем безопасности	4
Тема 3.2. СЗИ от НСД	***Лекции***	***24***
	Лекция 3.2.1. 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.	6
	Лекция 3.2.2. 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.	6
	Лекция 3.2.3. Обеспечение целостности информационной системы и информации	6
	Лекция 3.2.4. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.	6
	Практические занятия	***32***
	Практическое занятие 3.2.1. Установка и настройка СЗИ от НСД	4
	Практическое занятие 3.2.2. Защита входа в систему (идентификация и аутентификация пользователей)	4
	Практическое занятие 3.2.3. Разграничение доступа к устройствам	4
	Практическое занятие 3.2.4. Управление доступом	4
	Практическое занятие 3.2.5. Использование принтеров для печати конфиденциальных документов. Контроль печати	4
	Практическое занятие 3.2.6. Настройка системы для задач аудита	4
	Практическое занятие 3.2.7. Настройка контроля целостности и замкнутой программной среды	4
	Практическое занятие 3.2.8. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	4
	Самостоятельная работа обучающихся	***4***

	3.2.1. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации	4
Тема 3.3. Эксплуатация средств защиты информации в компьютерных сетях	***Лекции***	***48***
	Лекция 3.3.1. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	12
	Лекция 3.3.2. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	12
	Лекция 3.3.3. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	12
	Лекция 3.3.4. Настройка и устранение неисправности программно- аппаратных средств защиты информации в компьютерных сетях по заданным правилам	12
	Практические занятия	***2***
	Практическое занятие 3.3.1 Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2
Тема 3.4. Документация на защищаемую автоматизированную систему	***Лекции***	***10***
	Лекция 3.4.1. 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.	10
	Практические занятия	***8***
	Практическое занятие 3.4.1. Оформление основных эксплуатационных документов на автоматизированную систему.	8
	Курсовая работа(проект)	
	Консультации	***1***
МДК.01.02. Эксплуатация компьютерных сетей		**112**
Раздел 1. Основы передачи данных в компьютерных сетях		38
Тема 1.1. Модели сетевого взаимодейст вия	Содержание	2
	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 практических занятий и лабораторных работ	2
	Изучение элементов кабельной системы.	
Тема 1.2. Физический	Содержание	2
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	

уровень модели OSI	Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	
	Оптоволоконные линии связи	
	Стандарты кабелей. Электрическая проводка.	
	Беспроводная среда передачи.	
	Тематика практических занятий и лабораторных работ	4
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	
	Сварка оптического волокна	
Тема 1.3. Топология компьютерных сетей	Содержание	2
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий.	
	Тематика практических занятий и лабораторных работ	4
	Разработка топологи сети небольшого предприятия	
	Построение одноранговой сети	
Тема 1.4. Технологии Ethernet	Содержание	2
	Обзор технологий построения локальных сетей.	
	Технология Ethernet. Физический уровень.	
	Технология Ethernet. Канальный уровень	
	Тематика практических занятий и лабораторных работ	4
	Изучение адресации канального уровня. MAC-адреса.	
Тема 1.5. Технологии коммутации	Содержание	4
	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 практических занятий и лабораторных работ	2
	Создание коммутируемой сети	
Тема 1.6. Сетевой протокол IPv4	Содержание	4
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	
	Маршрутизация пакетов IPv4	
	Протоколы динамической маршрутизации	
	Тематика практических занятий и лабораторных работ	2
	Изучение IP-адресации.	
Тема 1.7.	Содержание	2

Скоростныеи беспроводные сети	Сеть FDDI. Сеть 100VG-AnyLAN Сверхвысокоскоростные сети Беспроводные сети	
	Тематика практических занятий и лабораторных работ	2
	Настройка беспроводного сетевого оборудования	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet		66
Тема 2.1.	Содержание	4
Основы коммутации	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 практических занятий и лабораторных работ	2
	Работа с основными командами коммутатора.	
Тема 2.2. Начальная настройка коммутатора	Содержание	2
	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 практических занятий и лабораторных работ	4
	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	2
	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 практических занятий и лабораторных работ	6
	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	4
	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 практических занятий и лабораторных работ	4
	Настройка протоколов связующего дерева STP, RSTP, MSTP.	
	Настройка функции защиты от образования петель LoopBackDetection	
	Агрегирование каналов.	
Тема 2.5. Адресация сетевогоуровня и маршрутизация	Содержание	4
	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 практических занятий и лабораторных работ	6
	Основные конфигурации маршрутизатора.	2
	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	4
	Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	
	Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	
	Тематика практических занятий и лабораторных работ	2
	Настройка QoS. Приоритизация трафика. Управление полосой пропускания	
Тема 2.7. Функции обеспечения безопасности и	Содержание	4
	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 практических занятий и лабораторных работ	2

ограничения доступа ксети	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	4
	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 практических занятий и лабораторных работ	4
	Отслеживание трафика многоадресной рассылки.	
	Отслеживание трафика Multicast	
Тема 2.9. Функции управления коммутаторами	Содержание	2
	Управление множеством коммутаторов. Протокол SNMP.	
	RMON (Remote Monitoring). Функция Port Mirroring.	
	Тематика практических занятий и лабораторных работ	4
	Функции анализа сетевого трафика.	
	Настройка протокола управления топологией сети LLDP.	
Раздел 3. Межсетевые экраны		16
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	Содержание	2
	Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	
	Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны.Криптографические механизмы безопасности.	
Тема 3.2. Межсетевые экраны	Содержание	2
	Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	
	Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	
	Тематика практических занятий и лабораторных работ	4
	Основы администрирования межсетевого 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 обнаружениями предотвращения проникновений	Содержание	2
	Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	
	Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	
	Тематика практических занятий и лабораторных работ	2
	Обнаружение и предотвращение вторжений.	
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	Содержание	2
	Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	
	Тематика практических занятий и лабораторных работ	2
	Создание альтернативных маршрутов с использованием статической маршрутизации	
МДК 01.03 Сети и системы передачи информации		
Раздел 1.Общие сведения о сетях и системах передачи информации		
Тема 1.1. Типы сетей.	**Содержание учебного материала**	**9**
	Виды сетей. Основные составляющие сети. Основные понятия и определения Понятие протокола. Иерархия протоколов. Интерфейсы и сервисы. Обобщенная структурная схема сети. Методы коммутации информации в сетях связи Основные технологии сетей передачи данных. Стандартизирующие организации	*4*
	Практические занятия/ Лабораторные занятия	*4*
	1. Виды сетей. 2. Основные составляющие сети. 3. Основные понятия и определения 4. Понятие протокола. 5. Иерархия протоколов. 6. Интерфейсы и сервисы. 7. Обобщенная структурная схема сети. 8. Методы коммутации информации в сетях связи 9. Основные технологии сетей передачи данных. 10. Стандартизирующие организации	
	Консультации	

	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*1*
Тема 1.2 Сетевые топологии.	**Содержание учебного материала**	**9**
	Общегосударственная система автоматической телефонной связи. Построение городских и сельских телефонных сетей. Архитектура и классификация телекоммуникационных сетей. Особенности защищенных телекоммуникационных сетей. Стандартизация телекоммуникационных сетей. Стратегии межсетевого взаимодействия.	*4*
	Практические занятия/ Лабораторные занятия	*4*
	1. Общегосударственная система автоматической телефонной связи. 2. Построение городских и сельских телефонных сетей. 3. Архитектура и классификация телекоммуникационных сетей. 4. Особенности защищенных телекоммуникационных сетей. 5. Стандартизация телекоммуникационных сетей. 6. Стратегии межсетевого взаимодействия.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*1*
Тема 1.3. Стандартные стеки коммуникационных протоколов.	**Содержание учебного материала**	**9**
	1. TCP/IP. 2. IPX/SPX	*4*
	Лабораторные занятия. 1. Определение затрат при создании ЛВС. 2. Основы монтажа сети. 3. Установка и настройка протокола TCP/IP. 4. Подключение к сети Internet, настройка клиента электронной почты. 5. Применение типовых схем при проектировании КС. 6. Определение технического состояния КС.	*4*
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*1*
Раздел 2. Уровни сетевого взаимодействия		
Тема 2.1. Физический уровень	**Содержание учебного материала**	**9**
	Среда передачи. Коаксиальный кабель. Витая пара. Оптоволокно. Структурированная кабельная система. Активное сетевое оборудование. Модуляция сигналов. Амплитудная модуляция. Частотная модуляция. Фазовая модуляция. Технология расширенного спектра Кодирование сигнала.	*4*

	Практические занятия/ Лабораторные занятия: 1. Среда передачи. 2. Коаксиальный кабель. 3. Витая пара. 4. Оптоволокно. 5. Структурированная кабельная система. 6. Активное сетевое оборудование. 7. Модуляция сигналов. 8. Амплитудная модуляция. 9. Частотная модуляция. 10. Фазовая модуляция. 11. Технология расширенного спектра 12. Кодирование сигнала.	*4*
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*1*
Тема 2.2. Канальный уровень	**Содержание учебного материала**	**9**
	Доступ к среде. Группа стандартов IEEE. Технология Ethernet. Сети с маркерным доступом. Технологии доступа с виртуальными каналами. Технологии беспроводного доступа. Технологии региональных сетей.	*4*
	Практические занятия/ Лабораторные занятия: 1. Доступ к среде. 2. Группа стандартов. 3. Технология Ethernet. 4. Сети с маркерным доступом. 5. Технологии доступа с виртуальными каналами. 6. Технологии беспроводного доступа. 7. Технологии региональных сетей.	*4*
	Консультации	
Тема 2.3. Транспортный уровень	**Содержание учебного материала**	**9**
	Основная концепция протоколов транспортного уровня. Протокол TCP. Формат пакета TCP. Управление потоком. Проблемы TCP. Протокол SCTP. Формат пакета SCTP. Множественность потоков и варианты доставки.	*4*
	Практические занятия/ Лабораторные занятия: 1. Основная концепция протоколов транспортного уровня. 2. Протокол TCP. 3. Формат пакета TCP. 4. Управление потоком.	*4*

	5. Проблемы TCP. Протокол SCTP. 6. Формат пакета SCTP. 7. Множественность потоков и варианты доставки.	
	Консультации	
Тема 2.4 Сетевой уровень	**Содержание учебного материала**	**9**
	Протокол IPv4. Формат пакета IP. Схема адресации протокола IPv4. Другие протоколы межсетевого уровня стека TCP/IP. Протокол RARP. Протокол ARP. Протокол ICMP	*4*
	Практические занятия/ Лабораторные занятия: 1. Протокол IPv4. 2. Формат пакета IP. 3. Схема адресации протокола IPv4. 4. Другие протоколы межсетевого уровня стека TCP/IP. 5. Протокол RARP. 6. Протокол ARP. **7.** Протокол ICMP	*4*
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*1*
Раздел 3. Построение локальной сети		
Тема 3.1. Сетевые устройства	**Содержание учебного материала**	**5**
	Структурированная кабельная система. Сетевые адаптеры. Концентраторы. Коммутаторы. Мосты. Шлюзы. Маршрутизаторы.	*2*
	Практические занятия/ Лабораторные занятия: 1. Структурированная кабельная система. 2. Сетевые адаптеры. 3. Концентраторы. 4. Коммутаторы. 5. Мосты. 6. Шлюзы. 7. Маршрутизаторы.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*1*
	Содержание учебного материала	**5**
	Структурированная кабельная система. Сетевые адаптеры. Концентраторы. Коммутаторы. Мосты. Шлюзы. Маршрутизаторы.	*2*

Тема 3.2. Логическая структуризация сети.	**Содержание учебного материала**	**5**
	Базовые технологии локальных сетей. Логическая структуризация сети.	*2*
	Практические занятия/ Лабораторные занятия: 1. Базовые технологии локальных сетей 2. Логическая структуризация сети.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*1*
Тема 3.3. Типовые схемы применения сетевого оборудования	**Содержание учебного материала**	**5**
	Установка и конфигурирование сетевого оборудования. Типовые схемы применения сетевого оборудования	*2*
	Практические занятия/ Лабораторные занятия: 1. Установка и конфигурирование сетевого оборудования. 2. Типовые схемы применения сетевого оборудования.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
Тема 3.4. Беспроводные и виртуальные локальные сети	**Содержание учебного материала**	**5**
	Беспроводные локальные сети. Виртуальные локальные сети. Потребность в применении VLAN	*2*
	Практические занятия/ Лабораторные занятия: 1. Беспроводные локальные сети. 2. Виртуальные локальные сети. 3. Потребность в применении VLAN.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Раздел 4. Построение глобальной сети		
Тема 4.1. Структура и функции глобальной сети	**Содержание учебного материала**	**5**
	Обобщенная структура и функции. Назначение и структура сетей. Интерфейсы глобальных сетей.	*2*
	Практические занятия/ Лабораторные занятия: 1. Обобщенная структура и функции. 2. Назначение и структура сетей. 3. Интерфейсы глобальных сетей.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа:	*1*

	Подготовить доклад по теме.	
Тема 4.2. Типы глобальных сетей	**Содержание учебного материала**	**5**
	Сети выделенных каналов. Сети с коммутацией каналов. Сети с коммутацией пакетов.	*2*
	Практические занятия/ Лабораторные занятия: 1. Сети выделенных каналов. 2. Сети с коммутацией каналов. 3. Сети с коммутацией пакетов.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 4.3. Коммутация в глобальных сетях	**Содержание учебного материала**	***5***
	Коммутация каналов. Коммутация сообщений и пакетов	*2*
	Практические занятия/ Лабораторные занятия: 1. Коммутация каналов. 2. Коммутация сообщений и пакетов	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 4.4. Базовые технологии глобальных протоколов	**Содержание учебного материала**	**6**
	Технология ARPANET. NSF. Другие сетевые технологии	*2*
	Практические занятия/ Лабораторные занятия: 1. Технология ARPANET. 2. NSF. 3. Другие сетевые технологии	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Тема 4.5. Удаленный доступ	**Содержание учебного материала**	***5***
	Организация удаленного доступа. Обзор программного обеспечения.	*2*
	Практические занятия/ Лабораторные занятия: 1. Организация удаленного доступа. 2. Обзор программного обеспечения.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Раздел 5. Защита информации в компьютерных сетях		

Тема 5.1. Защита информации в проводных сетях	**Содержание учебного материала**	**9**
	Брандмауэры с фильтрацией пакетов. Анализ сетевого трафика. Фильтрация на прикладном уровне и другие защитные функции. Защита сетевой ОС.	*4*
	Практические занятия/ Лабораторные занятия: 1. Брандмауэры с фильтрацией пакетов. 2. Анализ сетевого трафика. 3. Фильтрация на прикладном уровне и другие защитные функции. 4. Защита сетевой ОС.	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с учебной литературой, выполнение домашнего задания.	*1*
Тема 5.2. Защита информации в беспроводных сетях.	**Содержание учебного материала**	**5**
	Основные виды защиты. Технологии WPA и WEP.	*2*
	Практические занятия/ Лабораторные занятия: 1. Настройка брандмауэра. 2. Установка и настройка FTP -сервера. 3. Доступ к серверу по протоколу FTP. 4. Создание учетных записей и групп пользователей. 5. Создание политик групп пользователей. 6. Установка и настройка DNS – сервера, DHCP-сервера и HTTP-сервера	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Раздел 6. Техническая поддержка КС		
Тема 6.1. Обеспечение работоспособности КС.	**Содержание учебного материала**	**5**
	Основные характеристики работоспособности сети. Мероприятия по обеспечению работоспособности сети.	*2*
	Практические занятия/ Лабораторные занятия: 1. Основные характеристики работоспособности сети. 2. Мероприятия по обеспечению работоспособности сети.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 6.2. Техническая	**Содержание учебного материала**	**5**
	Техническая поддержка аппаратного обеспечения. Техническая поддержка программного обеспечения.	*2*

поддержка локальных сетей	**Практические занятия/ Лабораторные занятия:** 1. Техническая поддержка аппаратного обеспечения. 2. Техническая поддержка программного обеспечения.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 6.3. Определение качественного состояния кабельных линий.	**Содержание учебного материала**	**5**
	Структурированная кабельная система. Мероприятия по определению и обеспечению качественного состояния кабельных линий.	*2*
	Практические занятия/ Лабораторные занятия: 1. Структурированная кабельная система. 2. Мероприятия по определению и обеспечению качественного состояния кабельных линий.	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 6.4. Определение технического состояния КС.	**Содержание учебного материала**	**6**
	Определение технического состояния основных блоков сети. Коэффициент для оценки технического состояния КС.	*2*
	Практические занятия/ Лабораторные занятия: 1. Определение технического состояния основных блоков сети. 2. Коэффициент для оценки технического состояния КС.	*2*
	Консультации	*1*
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
МДК 01.04 Антивирусные системы		
Раздел 1. Методы защиты от вирусов и других вредоносных программных объектов		
Тема 1.1 Классификация компьютерных вирусов	**Содержание учебного материала**	**8**
	Типы вредоносных программ. Общее определение компьютерного вируса Различные типы вирусов Файловые вирусы Загрузочные вирусы Файлово-загрузочные вирусы	*2*

	Стелс-вирусы Шифрующиеся вирусы Полиморфные вирусы Макрокомандные вирусы Почтовые вирусы Вирусы в пакетных файлах ОС Вирусы в драйверах ОС Бестелесные вирусы Вирусы для пиринговых сетей Комбинированные вирусы Известные и неизвестные вирусы Коллекционные вирусы	
	Практические занятия/ Лабораторные занятия	*4*
	1. Типы вредоносных программ. 2. Общее определение компьютерного вируса 3. Различные типы вирусов 4. Файловые вирусы 5. Загрузочные вирусы 6. Файлово-загрузочные вирусы 7. Стелс-вирусы 8. Шифрующиеся вирусы 9. Полиморфные вирусы 10. Макрокомандные вирусы 11. Почтовые вирусы 12. Вирусы в пакетных файлах ОС 13. Вирусы в драйверах ОС 14. Бестелесные вирусы 15. Вирусы для пиринговых сетей 16. Комбинированные вирусы 17. Известные и неизвестные вирусы 18. Коллекционные вирусы	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.2 Классификация других вредоносных	**Содержание учебного материала**	**8**
	Логические бомбы Троянские объекты	*2*

программ	Троянские программы Троянские Web-сайты Троянские сообщения E-Mail Программы Backdoor Средства для получения несанкционированного доступа Техника Phishing Программы Spyware Программы Adware Клавиатурный шпион Комбинированные вредоносные программы	
	Практические занятия/ Лабораторные занятия	*4*
	1. Логические бомбы 2. Троянские объекты 3. Троянские программы 4. Троянские Web-сайты 5. Троянские сообщения E-Mail 6. Программы Backdoor 7. Средства для получения несанкционированного доступа 8. Техника Phishing 9. Программы Spyware 10. Программы Adware 11. Клавиатурный шпион 12. Комбинированные вредоносные программы	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.3. Способы распространения вредоносных программ	**Содержание учебного материала**	**7**
	Файлы исполняемых программ Файлы офисных документов Файлы интерпретируемых программ Загрузочные секторы дисков и дискет Сообщения электронной почты Файлообменные (пиринговые) сети	*2*
	Практические занятия/ Лабораторные занятия. 1. Файлы исполняемых программ 2. Файлы офисных документов 3. Файлы интерпретируемых программ	*4*

	4. Загрузочные секторы дисков и дискет 5. Сообщения электронной почты 6. Файлообменные (пиринговые) сети	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*1*
Тема 1.4. Вредоносное воздействие компьютерных вирусов	**Содержание учебного материала**	**8**
	Визуальные и звуковые эффекты Воздействие на файлы Изменение содержимого секторов диска Воздействие на базы данных Воздействие на аппаратное обеспечение компьютеров Воздействие на систему в целом Получение несанкционированного доступа и похищение информации Компрометация пользователя Социальный инжиниринг	*2*
	Практические занятия/ Лабораторные занятия: 1. Визуальные и звуковые эффекты 2. Воздействие на файлы 3. Изменение содержимого секторов диска 4. Воздействие на базы данных 5. Воздействие на аппаратное обеспечение компьютеров 6. Воздействие на систему в целом 7. Получение несанкционированного доступа и похищении информации 8. Компрометация пользователя 9. Социальный инжиниринг	*4*
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*2*
Тема 1.5. Обнаружение компьютерных вирусов и других вредоносных программ	**Содержание учебного материала**	**7**
	Сканирование Эвристический анализ Обнаружение изменений Анализ сетевого трафика Анализ баз данных почтовых программ Обнаружение вирусов в системе автоматизации документооборота Вакцинирование	*2*

	Практические занятия/ Лабораторные занятия: 1. Сканирование 2. Эвристический анализ 3. Обнаружение изменений 4. Анализ сетевого трафика 5. Анализ баз данных почтовых программ 6. Обнаружение вирусов в системе автоматизации документооборота 7. Вакцинирование	*4*
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*1*
Тема 1.6. Типы антивирусных программ	**Содержание учебного материала**	**14**
	Сканеры Сканирование по запросу пользователя Сканирование при обращении к файлам Сканирование по расписанию Сканирование сетевого трафика Ревизоры диска Встроенные антивирусы	*4*
	Практические занятия/ Лабораторные занятия: 1. Сканеры 2. Сканирование по запросу пользователя 3. Сканирование при обращении к файлам 4. Сканирование по расписанию 5. Сканирование сетевого трафика 6. Ревизоры диска 7. Встроенные антивирус 8. Программа Kaspersky Anti-Virus 9. Программа Dr.Web 10. Программа Norton Antivirus 11. Прочие антивирусные программы 12. Программа Stop! 13. Программа Panda Antivirus 14. Программа Virus Scan	*8*
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*

Тема 1.7. Антивирусы для интрасетей и для интернета	**Содержание учебного материала**	**8**
	Проблемы защиты крупных корпоративных интрасетей Функции удаленного управления и контроля Удаленное обновление антивирусных баз данных Децентрализованная установка и обновление антивирусов с сетевым центром управления Удаленная настройка антивирусных программ Обнаружение новых рабочих станций Планирование заданий Сигнальное информирование Архитектура и принципы работы корпоративных систем антивирусной защиты	*2*
	Практические занятия/ Лабораторные занятия: 1. Проблемы защиты крупных корпоративных интрасетей 2. Функции удаленного управления и контроля 3. Удаленное обновление антивирусных баз данных 4. Децентрализованная установка и обновление антивирусов с сетевым центром управления 5. Удаленная настройка антивирусных программ 6. Обнаружение новых рабочих станций 7. Планирование заданий 8. Сигнальное информирование **9.** Архитектура и принципы работы корпоративных систем антивирусной защиты	*4*
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*
Раздел 2. Методы защиты деструктивного воздействия		
Тема 2.1. Установка и удаление программы Dr.Web для Windows	**Содержание учебного материала**	**7**
	Состав дистрибутива Сканер Dr.Web Сторож SpIDer Guard Почтовый сторож SpIDer Mail Планировщик заданий Утилита обновления Процедура установки пакета Dr.Web для Windows Удаление пакета Dr.Web для Windows	*2*
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива 2. Сканер Dr.Web 3. Сторож SpIDer Guard	*4*

	4. Почтовый сторож SpIDer Mail 5. Планировщик заданий 6. Утилита обновления 7. Процедура установки пакета Dr.Web для Windows 8. Удаление пакета Dr.Web для Windows	
	Консультации	
	Самостоятельная внеаудиторная работа:	*1*
Тема 2.2. Настройка пакета Dr.Web для Windows	**Содержание учебного материала**	**7**
	Стандартный пакет Dr.Web для Windows и пакет Dr.Web Home Edition Параметры проверки объектов Принципы отбора файлов для сканирования Настройка реакции программы на события Настройка ведения отчета Настройка звуковых реакций программы Настройка средств обновления Настройка системных установок	*2*
	Практические занятия/ Лабораторные занятия: 1. Стандартный пакет Dr.Web для Windows и пакет Dr.Web Home Edition 2. Параметры проверки объектов 3. Принципы отбора файлов для сканирования 4. Настройка реакции программы на события 5. Настройка ведения отчета 6. Настройка звуковых реакций программы 7. Настройка средств обновления 8. Настройка системных установок	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
Тема 2.3. Защита почтовых систем	**Содержание учебного материала**	**5**
	Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Параметры командной строки. Обнаружение вирусов Справочная система программы	*2*
	Практические занятия/ Лабораторные занятия: 1. Параметры командной строки 2. Обнаружение вирусов 3. Справочная система программы	*2*

	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
Тема 2.4. Почтовый антивирусный сторож SpIDer Mail	**Содержание учебного материала**	**5**
	Параметры командной строки Обнаружение вирусов Справочная система программы	*2*
	Практические занятия/ Лабораторные занятия: 1. Параметры командной строки 2. Обнаружение вирусов 3. Справочная система программы	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	
Тема 2.5. Антивирусный комплекс ESET Nod32/Ср/	**Содержание учебного материала**	**7**
	Состав дистрибутива пакета ESET Nod32/Ср/ Установка и удаление пакета ESET Nod32/Ср/ Требования к установленным программам Требования к конфигурации компьютера Особенности пакета ESET Nod32/Ср/ Конфигурация пакета ESET Nod32/Ср/ Удаление пакета ESET Nod32/Ср/ Ознакомительная версия пакета Dr.Web для Unix Установка файла регистрационного ключа Обновление пакета ESET Nod32/Ср/ для Unix Вирусные базы данных пакета ESET Nod32/Ср/ для Unix	*2*
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива пакета ESET Nod32/Ср/ 2. Установка и удаление пакета ESET Nod32/Ср/ 3. Требования к установленным программам 4. Требования к конфигурации компьютера 5. Особенности пакета ESET Nod32/Ср/ 6. Конфигурация пакета ESET Nod32/Ср/ 7. Удаление пакета ESET Nod32/Ср/	*4*

	8. Ознакомительная версия пакета Dr.Web для Unix 9. Установка файла регистрационного ключа 10. Обновление пакета ESET Nod32/Ср/ для Unix 11. Вирусные базы данных пакета ESET Nod32/Ср/ для Unix	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.6. Мобильные антивирусы: защита планшетов и телефонов	**Содержание учебного материала**	**7**
	Запуск сканера Параметры командной строки Параметры проверки объектов Действия при обнаружении вирусов Принципы отбора файлов для сканирования Настройка реакции сканера на события Настройка ведения отчета	*2*
	Практические занятия/ Лабораторные занятия: 1. Запуск сканера 2. Параметры командной строки 3. Параметры проверки объектов 4. Действия при обнаружении вирусов 5. Принципы отбора файлов для сканирования 6. Настройка реакции сканера на события 7. Настройка ведения отчета	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.7. Защита серверов и рабочих станций Kaspersky 6.0 для Windows	**Содержание учебного материала**	***7***
	Состав дистрибутива Установка и настройка Требования к операционной системе Требования к установленным программам Требование к квалификации пользователя Процесс установки Конфигурация Kaspersky 6.0 для Windows Параметры проверки объектов Принципы отбора файлов для сканирования Настройка реакции программы на события	*2*

	Настройка ведения отчета Настройка реакций программы Настройка средств обновления Удаление Kaspersky 6.0 для Windows	
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива 2. Установка и настройка 3. Требования к операционной системе 4. Требования к установленным программам 5. Требование к квалификации пользователя 6. Процесс установки 7. Конфигурация Kaspersky 6.0 для Windows 8. Параметры проверки объектов 9. Принципы отбора файлов для сканирования 10. Настройка реакции программы на события 11. Настройка ведения отчета 12. Настройка реакций программы	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.8. Антивирусные решения компании Sophos	**Содержание учебного материала**	***7***
	Состав дистрибутива Установка пакета Sophos Small Business Suite Первый этап установки Второй этап установки Установка вручную Установка на компьютеры, не подключенные к Интернету Просмотр состояния антивирусной защиты на узлах сети Добавление новых компьютеров Обновление антивирусов и антивирусной базы данных Проверка файлов в автоматическом режиме Удаление вирусов Настройка извещений о вирусном заражении Настройка параметров антивирусной защиты рабочих станций Настройка параметров сканирования Настройка параметров удаления вирусов Настройка параметров антивирусной проверки	*2*

	Исключение файлов и дисков из проверки	
	Практические занятия/ Лабораторные занятия: 4. Состав дистрибутива 5. Установка пакета Sophos Small Business Suite 6. Первый этап установки 7. Второй этап установки 8. Установка вручную 9. Установка на компьютеры, не подключенные к Интернету 10. Просмотр состояния антивирусной защиты на узлах сети 11. Добавление новых компьютеров 12. Обновление антивирусов и антивирусной базы данных 13. Проверка файлов в автоматическом режиме 14. Удаление вирусов 15. Настройка извещений о вирусном заражении 16. Настройка параметров антивирусной защиты рабочих станций 17. Настройка параметров сканирования 18. Настройка параметров удаления вирусов 19. Настройка параметров антивирусной проверки 20. Исключение файлов и дисков из проверки	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Примерная тематика курсовых работ Физическое кодирование с использованием манчестерского кода Логическое кодирование с использованием скремблирования Подключение клиента к беспроводной сети в инфраструктурном режиме Оценка беспроводной линии связи Проектирования беспроводной сети Сбор информации о клиентских устройствах Планирование производительности и зоны действия беспроводной сети Предпроектное обследование места установки беспроводной сети Обеспечение отказоустойчивости в беспроводных сетях Режимы работы и организация питания точек доступа Сегментация беспроводной сети Настройка QoS Постпроектное обследование и тестирование сети Создание ACL-списка		

Наблюдение за трафиком в сети VLAN Определение уязвимых мест сети Реализация функций обеспечения безопасности порта коммутатора Исследование трафика Создание структуры сети организации Определение технических требований Мониторинг производительности сети Создание диаграммы логической сети Подготовка к обследованию объекта Обследование зоны беспроводной связи Формулировка общих целей проекта Разработка требований к сети Анализ существующей сети Определение характеристик сетевых приложений Анализ сетевого трафика Определение приоритетности трафика Изучение качества обслуживания сети Исследование влияния видеотрафика на сеть Определение потоков трафика, построение диаграмм потоков трафика Применение проектных ограничений Определение проектных стратегий для достижения масштабируемости Определение стратегий повышения доступности Определение требований к обеспечению безопасности Разработка ACL-списков для реализации наборов правил межсетевого экрана Использование CIDR для обеспечения объединения маршрутов Определение схемы IP-адресации 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 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	
Производственная практика	***144 ч***
Всего	***876 ч***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПМ

3.1. Требования к минимальному материально-техническому обеспечению

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Практические занятия проводятся в кабинете интернет-технологий и информатики, оборудованным ПЭВМ с установленным программным обеспечением:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- система программирования «Microsoft Visual Studio Express»;
- программа просмотра pdf-документов Sumatra PDF Reader.

Для самостоятельной работы студентов используется кабинет интернет-технологий и информатики.
Оснащение кабинета:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
- ОС Microsoft Windows
- Антивирус Касперского
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Производственная практика проводятся при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализовываются как в несколько периодов, так и рассредоточено, чередуясь с теоретическими занятиями в рамках профессиональных модулей.

Производственная практика проводится на предприятиях (в организациях) города и района. Оборудование предприятий (организаций) и технологическое оснащение рабочих мест производственной практики соответствует содержанию деятельности и дает возможность обучающемуся овладеть профессиональными компетенциями по всем осваиваемым видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Для реализации программы библиотечный фонд имеет печатные, электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Учебники и учебные пособия по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем находятся в свободном доступе для преподавателей и студентов в библиотеке Колледжа ДГУ, в том числе электронные издания на официальном сайте Колледжа ДГУ. Библиотека колледжа оборудована рабочими местами в читальном зале и выходом в Интернет для работы с электронными книгами, учебниками, учебными пособиями, размещёнными на сайте Колледжа ДГУ. В колледже созданы все условия, позволяющие широко использовать в образовательном процессе информационные технологии, своевременно обеспечивать обновление нормативной документации, необходимой информации и оперативный доступ к ней.

Колледж имеет выход в Интернет, работает электронная почта, созданы и поддерживаются сайты (официальный сайт ДГУ - www.dgu.ru), официальный сайт Колледжа ДГУ (http:/law.dgu.ru/college/).

Основная литература:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — URL : https://urait.ru/bcode/491456
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего

профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2022. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — URL : https://urait.ru/bcode/491951
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — URL : https://urait.ru/bcode/476997
4. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — URL : https://urait.ru/bcode/495353

Дополнительная литература:

1. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва: Издательство Юрайт, 2021. - 363 с. - (Профессиональное образование).- ISBN 978-5-9916-0480-2 .- Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/475704.
2. Имитационное моделирование : учебное пособие для среднего профессионального образования / Ю. Г. Древс, В. В. Золотарёв. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 142 с. — (Профессиональное образование). — ISBN 978-5-534-11951-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475680 (дата обращения: 22.12.2021).
3. Сети и системы передачи информации: телекоммуникационные сети: учебник и практикум для академического бакалавриата / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва : Издательство Юрайт, 2016. - 363 с. - (Бакалавр. Академический курс). - ISBN 978-5-9916-7198-9. - Текст: электронный //Образовательная платформа Юрайт [сайт]. -URL: https://urait.ru/bcode/391942.
4. Берикашвили, В. Ш. Основы радиоэлектроники: системы передачи информации: учебное пособие для среднего профессионального образования / В. Ш. Берикашвили. - 2-е изд., испр. и доп. - Москва: Издательство Юрайт, 2019. - 105 с. - (Профессиональное образование). - ISBN 978-5-534-10493-6. - Текст: электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/430609.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения ПМ

1. ЭБС «Университетская библиотека ONLINE». – URL: www.biblioclub.ru
2. ЭБС издательства «Лань». – URL: https://e.lanbook.com
3. ЭБС «ZNANIUM.COM» www.znanium.com

4. Электронный каталог Научной библиотеки КубГУ. – URL:http://212.192.134.46/MegaPro/Catalog/Home/Index Электронная библиотека «Издательского дома «Гребенников» - URL:www.grebennikon.ru
6. Научная электронная библиотека (НЭБ) «eLibrary.ru». - URL:http://www.elibrary.ru
7. Базы данных компании «Ист Вью». - URL:http://dlib.eastview.com
8. Лекториум ТВ». - URL: http://www.lektorium.tv/
9. Национальная электронная библиотека «НЭБ». - URL:http://нэб.рф/
10.КиберЛенинка: научная электронная библиотека. – URL: http://cyberleninka.ru/
11.Единое окно доступа к образовательным ресурсам : федеральная ИС свободного доступа. – URL: http://window.edu.ru.
12.Справочно-правовая система «Консультант Плюс» - URL http://www.consultant.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПМ

Контроль и оценка результатов освоения ПМ осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) системв защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно- аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике