АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ИНФОРМАЦИОННЫЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02.Эксплуатация и модернизация объектов сетевой инфраструктуры

2017

Организация-разработчик: АНО ПО «Балтийский информационный техникум»

Разработчики:

Балаклиевский Валерий Давидович, зам. Директора АНО ПО «БИТ»,

Славинская Т.В, председатель ЦМК № 2 АНО ПО «БИТ»

Рассмотрена на заседании цикловой методической комиссии «Информационных технологий» 27 февраля 2017г.

СОДЕРЖАНИЕ *СТР.*

1. *ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ*

ПМ.02.Эксплуатация и модернизация объектов сетевой инфраструктуры

1.1. Область применения рабочей программы

Рабочая программа (Далее программа) профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО **09.02.06 «Сетевое и системное администрирование»**, базовый уровень подготовки, укрупненная группа направления 09.00.00 Информатика и вычислительная техника в части освоения основного вида профессиональной деятельности): **Организация сетевого администрирования** и соответствующих профессиональных компетенций:

ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2. Администрировать сетевые ресурсы в информационных системах.
ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Программа профессионального модуля может быть использована **в** дополнительном профессиональном образовании и профессиональной подготовке работников в области информатики и вычислительной техники при наличии среднего общего образования.

1.2. Цели и задачи профессионального модуля - требования к результатам освоения профессионального модуля МДК02.01, Раздел 1: «Организация сетевого администрирования».

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

иметь практический опыт в:
- установке, настройке и сопровождении, контроле использования сервера и рабочих станций для безопасной передачи информации.

уметь:
- проектировать локальную сеть, выбирать сетевые топологии;
- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".

знать:
- основные направления администрирования компьютерных сетей;
- утилиты, функции, удаленное управление сервером;
- технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.

1.2.1 Цели и задачи профессионального модуля - требования к результатам освоения профессионального модуля МДК02.01, Раздел 2: «Сопровождение модернизации сетевой инфраструктуры».

Освоение профессионального модуля направлено на развитие общих компетенций:

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.

Освоение профессионального модуля «Сопровождение модернизации сетевой инфраструктуры» и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.
ПК 3.4 Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

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

иметь практический опыт в:

-настройке, планировании и поддержке сетевой инфраструктуры;
-структурировании и выделении модулей сети, разработке сетевых топологий в соответствии с требованиями отказоустойчивости и повышения производительности корпоративной сети.

уметь:

- планировать и поддерживать сетевую инфраструктуру;
- оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.

знать:

- функциональные возможности системного программного обеспечения с учетом новых версий;

- основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.

1.2.2 Цели и задачи профессионального модуля - требования к результатам освоения профессионального модуля МДК.02.02, Раздел 1: «Защита от угроз из Интернет».

Освоение профессионального модуля «Защита от угроз из Интернета» и соответствующих профессиональных компетенций (ПК):

ПК. 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4. Принимать участие в приемо- сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
ПК 1.5. Выполнять требования нормативно- технической документации, иметь опыт оформления проектной документации.

Цели и задачи раздела междисциплинарного курса - требования к результатам освоения: в результате изучения раздела междисциплинарного курса студент должен:

***Иметь представление*:**

- об основах проектирования и практических реализациях сетей масштаба предприятия;
- о современных методах и технологиях защиты информации в корпоративных сетях;

Знать:

- терминологию в области безопасности корпоративных сетей;
- методологию построения безопасных корпоративных сетей;
- современные сетевые технологии и сервисы;

Уметь:

- анализировать угрозы безопасности корпоративной сети;
- разрабатывать и реализовывать предложения по созданию системы защиты для конкретных корпоративных сетей;

1.2.3 Цели и задачи профессионального модуля - требования к результатам освоения профессионального модуля МДК.02.02, Раздел 2: «Основы компьютерной безопасности».

Освоение профессионального модуля «Основы компьютерной безопасности» и соответствующих профессиональных компетенций (ПК):

ПК. 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4. Принимать участие в приемо- сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
ПК 1.5. Выполнять требования нормативно- технической документации, иметь опыт оформления проектной документации.

Цели и задачи раздела междисциплинарного курса - требования к результатам освоения:

В результате изучения раздела междисциплинарного курса студент должен:

Знать:

- наиболее важные аспекты проблем безопасности компьютерных технологий;
- основные средства и методы защиты компьютерной информации;
- основные пакеты прикладных программ по защите информации;

Уметь:

- устанавливать, обслуживать, применять средства защиты информации от НСД;
- обеспечивать защиту информации и управление доступом к информационным ресурсам в информационных системах.

1.2.4 Цели и задачи профессионального модуля - требования к результатам освоения профессионального модуля МДК.02.02, Раздел 3: «Защита информации в Компьютерных сетях».

Освоение профессионального модуля «Защита информации в Компьютерных сетях» и соответствующих профессиональных компетенций (ПК):

ПК. 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4. Принимать участие в приемо- сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
ПК 1.5. Выполнять требования нормативно- технической документации, иметь опыт оформления проектной документации.

Целью дисциплины: «Защита информации в компьютерных сетях» является формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи дисциплины – дать знания:

- о методах и средствах защиты информации в компьютерных сетях;
- о технологии межсетевого экранирования;
- о методах и средствах построения виртуальных частных сетей;
- о методах и средствах аудит уровня защищенности информационных систем.

Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности.

В результате изучения дисциплины студенты должны

знать:

• технологии обнаружения компьютерных атак и их возможности;

• основные уязвимости и типовые атаки на современные компьютерные системы;

• возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;

• методы защиты компьютерных сетей;

• классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;

• основные принципы администрирования защищенных компьютерных систем;

• особенности реализации методов защиты информации современными программно-аппаратными средствами;

уметь:

• выполнять функции администратора безопасности защищенных компьютерных систем;

• выполнять настройку защитных механизмов сетевых программно-аппаратных средств;

• настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;

• применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;

• организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;

владеть

• средствами администрирования сетевых программно-аппаратных комплексов защиты информации;

• средствами администрирования систем обнаружения компьютерных атак;

• средствами и системами аудита информационной безопасности;

• методикой проведения аудита информационной безопасности

• средствами администрирования систем организации виртуальных частных сетей.

Содержание профессионального модуля состоит из набора разделов, каждый из которых соответствует конкретной профессиональной компетенции или нескольким компетенциям и направлен на развитие набора универсальных компетенций.

Дескрипторы сформированности компетенций по разделам профессионального модуля.

Спецификация ПК/ разделов1,2 профессионального модуля ПМ.01

Формируемые компетенции	***Название раздела***		
	Действия (дескрипторы)	***Умения***	***Знания***
МДК 02.01. ***Раздел модуля: «Организация сетевого администрирования»***			
ОК 01. Выбирать способы	*Решать задачи*	Распознавать задачу и/или проблему в	основные источники

решения задач профессиональной деятельности, применительно к различным контекстам.	*профессиональной деятельности*	профессиональном и/или социальном контексте; Анализировать задачу и/или проблему и выделять её составные части; Правильно определить и найти информацию, необходимую для решения задачи и/или проблемы;	информации и ресурсов для решения задач и проблем в профессиональном и/или социальном контексте. актуальные стандарты выполнения работ в профессиональной и смежных областях;
ОК 03. Планировать и реализовывать собственное и профессиональное и личностное развитие.	*Решать задачи профессиональной деятельности*	Определять актуальность нормативно-правовой документации в профессиональной деятельности	Содержание актуальной нормативно-правовой документации
ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.	администрировать локальную сеть в соответствии с поставленной задачей	администрировать локальные вычислительные сети	основные направления администрирования компьютерных сетей утилиты, функции, удаленное управление сервером;
ПК 2.2. Администрировать сетевые ресурсы в информационных системах.	администрировать локальную сеть в соответствии с поставленной задачей	администрировать локальные вычислительные сети; принимать меры по устранению возможных сбоев;	основные направления администрирования компьютерных сетей
ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.	администрировать локальную сеть в соответствии с поставленной задачей	принимать меры по устранению возможных сбоев;	основные направления администрирования компьютерных сетей;
МДК 02.01 ***Раздел модуля 2: «Сопровождение модернизации сетевой инфраструктуры»***			

ПКЗ.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	Настраивать, планировать и поддерживать сетевую инфраструктуру; Структурировать и выделять модули сети, разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производитель-ности сети	оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.	функциональные возможности системного программного обеспечения с учетом новых версий
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	Настраивать, планировать и поддерживать сетевую инфраструктуру; Структурировать и выделять модули сети, разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производи-тельности	планировать и поддерживать сетевую инфраструктуру;	основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.
ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.	Настраивать, планировать и поддерживать сетевую инфраструктуру; Структурировать и выделять модули сети, разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производитель-	планировать и поддерживать сетевую инфраструктуру; оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.	основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.

	ности корпоративной сети		
ПК 3.4 Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.	Настраивать, планировать и поддерживать сетевую инфраструктуру; Структурировать и выделять модули сети, разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производитель-ности корпоративной сети	планировать и поддерживать сетевую инфраструктуру; оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.	функциональные возможности системного программного обеспечения с учетом новых версий; основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.	Настраивать, планировать и поддерживать сетевую инфраструктуру;	планировать и поддерживать сетевую инфраструктуру; оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.	функциональные возможности системного программного обеспечения с учетом новых версий; основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	Структурировать и выделять модули сети, разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производитель-ности корпоративной сети	оптимизировать работу сервера и устранять неполадки с помощью инструментальных средств.	основы методологии дизайна архитектуры сети, в том числе с использованием «периметра», модульный подход к дизайну.

Спецификация ПК/ разделов 1, 2, 3 профессионального модуля ПМ.02

Формируемые компетенции	***Название раздела***		
	Действия (дескрипторы)	***Умения***	***Знания***
МДК 02.02. ***Раздел модуля: «Защита от угроз из Интернета»***			

ПК. 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.	*Решать задачи профессиональной деятельности*	выполнять настройку защитных механизмов сетевых программно-аппаратных средств; настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации; применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;	возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;
ПК 1.4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.	*Решать задачи профессиональной деятельности*	выполнять функции администратора безопасности защищенных компьютерных систем;	технологии обнаружения компьютерных атак и их возможности; основные уязвимости и типовые атаки на современные компьютерные системы; методы защиты компьютерных сетей; основные принципы администрирования защищенных компьютерных систем;

ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.	*Решать задачи профессиональной деятельности*	организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;	особенности реализации методов защиты информации современными программно-аппаратными средствами; классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;

1.3 Рекомендуемое количество часов на освоение программы профессионального модуля ПМ.02:

максимальной учебной нагрузки обучающегося - **610** часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – **476** часов;
практическая работа – **140** часов;
курсовой проект – **30** часов;
самостоятельной работы обучающегося – **240** часов;
учебной практики -**72** часа;
производственной практики - **144** часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Тематический план профессионального модуля ПМ.01, МДК.02.01

Коды профессио-нальных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4	МДК 02.01 Раздел 1. Организация сетевого администрирования	300	200	120	30	100		36	72
ПК 5.1; ПК 5.2; ПК 5.3; ПК 5.4; ПК 5.5	МДК.02.02 Защита от угроз из Интернета	420	280	140		140		36	72
ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4	ПП.02 Производственная практика(по профилю специальности)								144
	Всего:	936	480	160	30	240		72	144

2.1.1 Тематический план профессионального модуля ПМ.02, МДК. 02.02

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 1.3. ПК 1.4 ПК 1.5	**Раздел 1. Защита от угроз из Интернета**	100	80	40		46			
ПК 1.3. ПК 1.4 ПК 1.5	**Раздел 2. Основы компьютерной безопасности**	120	100	50		46			
ПК 1.3. ПК 1.4 ПК 1.5	**Раздел 3. Защита информации в компьютерных сетях**	120	100	50		46			
	Всего:	**360**	**280**	**140**		**140**			

2.2. Содержание обучения по профессиональному модулю (ПМ.01) «Организация сетевого администрирования»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ(проект)	Объем часов	Уровень освоения
1	**2**	**3**	**4**
МДК.02.01. Раздел 1. Организация сетевого администрирования		**200**	
Организация сетевого администрирования		**200**	
Введение	О программном обеспечении компьютерных сетей.	**2**	1
Тема 1.1. Установка WEB-сервера	**Содержание**	**60**	
	1. **Выбор аппаратной части.** Оперативная память. Диски.		2
	2. **Конфигурирование web-сервера.** Спецификация TCP портов. Взаимодействие с системой защиты. Корневой каталог сервера. Увеличение производительности. Ограничение потери ресурсов. Количество серверов. Создание индексов и/или поиск по индексам.		2
	3. **Запуск, перезапуск и остановка сервера.** Под управлением ОС Linux. Под управлением ОС Windows. Под управлением ОС Max ОС.		2
	4. **Хостинг нескольких web-узлов.** Домашние страницы пользователей. IP-адреса и порты. Виртуальный хостинг по имени. Настройка виртуального хостинга по имени. Виртуальный хостинг по IP-адресу.		2

	5.	**Регистрация и мониторинг.** Регистрация ошибок. Журнал регистрации и обмена данными. Модуль mod ststus. Проблемы с производительностью.		2
	6	**Безопасность.** Безопасность каталогов. Отключение автоматического индексирования. Отключение прав пользователей. Основы идентификации. Идентификация по пользователю. Контроль за групповым доступом. Определение действующих пользователей. Шифрование с открытым ключом. Сертификация.		2
	7.	**Динамические web-страницы.** Вставки на стороне сервера. Листинг вставок. Интерфейс CGI. Управление потреблением ресурсов. Взаимодействие между процессами.		2
	Практические занятия 1. Изучение дополнительных опций конфигурирования web-сервера 2. Изучение запуска, перезапуска и останов сервера под управлением ОС Max ОС. 3. Изучение хостинга нескольких web-узлов. 4. Изучение организации динамических web-страниц 5. Вставки на стороне сервера. Листинг вставок. Интерфейс CGI. Управление потреблением ресурсов. Взаимодействие между процессами.		2	
Тема 1.2. Установка и параметры брандмауэра.	**Содержание**			
	8.	**Установка брандмауэра.** Настройка ядра. Сборка пакета для установки. Установка пакета.		3
	9.	Порядок прохождения таблиц и цепочек. Общее положение. Таблица Mangle. Таблица Nat. Таблица Filter.		2
	10.	Механизм определения состояний. Таблица трассировщика. Состояния в пространстве пользователя. TCP соединения. UDP соединения. ICMP соединения. Поведение по умолчанию. Трассировка комплексных протоколов.		2

	11.	Сохранение и восстановление больших наборов правил. Плюсы и минусы. Iptables-save. Iptables-restore.		2
	12.	Как строить правила.		2

		Таблицы. Команды. Критерии. Общие критерии. Неявные критерии. Явные критерии. Критерий "мусора" (Unclean match).		
	13.	Действия и переходы. Действие ACCEPT. Действие DNAT. Действие DROP. Действие LOG. Действие ULOG.		2
	Практические занятия Установка брандмауэра. Порядок прохождения таблиц и цепочек. Механизм определения состояний. Сохранение и восстановление больших наборов правил. Построение правил. Действия и переходы.		2	
Тема 1.3. Настройка сервера и рабочих станций для безопасной передачи информации.	**Содержание**			
	14.	**Настройка службы DCHP Server.** Создание диапазона IP-адресов. Конфигурирование зарезервированных IP-адресов. Настройка DHCP-опций.		3
	15.	**Настройка службы DNS Server.** Создание зон. Настройка клиента службы DNS Server. Настройка процесса разрешения имен хостов с использованием службы DNS Server.		3
	16.	**Настройка информационной системы домена.** Установка и конфигурирование средств администрирования домена. Создание учетных записей пользователя. Создание групп. Управление членством в группе.		2
	17.	**Настройка групповых политик домена.** Управление применением групповых политик. Создание шаблона безопасности и использование его совместно с групповой политикой.		2
	18.	**Конфигурирование безопасной передачи информации.** Использование протоколов IPSec. Конфигурирование шифрующей файловой системы. Аутентификация с помощью службы RADIUS.		3

	Практические занятия Создание диапазона IP-адресов. Конфигурирование зарезервированных IP-адресов. Настройка DHCP-опций.	2	

	Создание зон. Настройка клиента службы DNS Server. Настройка процесса разрешения имен хостов с использованием службы DNS Server. Установка и конфигурирование средств администрирования домена. Создание учетных записей пользователя. Создание групп. Управление членством в группе. Управление применением групповых политик. Создание шаблона безопасности и использование его совместно с групповой политикой. Конфигурирование шифрующей файловой системы. Аутентификация с помощью службы RADIUS.		
Тема 1.4. Организация доступа к локальным и глобальным сетям	**Содержание**		
	19. **Основные принципы маршрутизации.** Логика работы маршрутизации. Статическая и динамическая маршрутизация. Настройка статической и динамической маршрутизации.		2
	20. **Организация доступа к сетям по беспроводному соединению.** Настройка оборудования Wi-Fi (точки доступа). Настройки на клиентских машинах. Создание профиля подключения.		2
	21. **Организация кэширующего proxy-сервера.** Настройка Access Control List. Использование аутентификации пользователей. Специфика использования иерархии прокси- серверов.		3
	22. **Обеспечение защиты при доступе к глобальным сетям.** Настройка брандмауэра (firewall); системы трансляции сетевых адресов (NAT); прозрачного проксирования (transparent proxy).		3
	Практические занятия: Настройка оборудования Wi-Fi (точки доступа). Настройки на клиентских машинах. Создание профиля подключения. Настройка Access Control List. Использование аутентификации пользователей. Специфика использования иерархии прокси- серверов. Настройка брандмауэра (firewall); системы трансляции сетевых ад-	2	

	ресов (NAT); прозрачного проксирования (transparent proxy).		
Тема 1.5. Сопровождение и контроль использования Web сервера, файлового сервера, почтового сервера, SQL -	**Содержание**		
	23. **Сопровождение и контроль Web сервера.** Контроль конфигурации сервера. Ограничение доступа к серверу. Оптимизация передачи данных. Обновление модулей и служб сервера.		2
	24. **Сопровождение и контроль файлового сервера.** Контроль конфигурации сервера. Настройка прав доступа пользователей к ресурсам. Обновление служб сервера.		2
	25. **Сопровождение и контроль почтового сервера.** Контроль отправки и приёма почты. Настройка прав доступа пользователей к почтовым аккаунтам. Обновление служб сервера.		2
	26. **Сопровождение и контроль SQL - сервера.** Контроль конфигурации сервера. Резервное копирование и восстановление баз данных. Настройка прав доступа пользователей к базам данных. Обновление служб сервера.		2
	27. **Оптимизация служб сервера.** Оптимизация производительности служб сервера. Оптимизация обмена данными со службой SQL - сервера. Оптимизация использования памяти службами.		2
	Практические занятия: Контроль конфигурации сервера. Ограничение доступа к серверу. Оптимизация передачи данных. Обновление модулей и служб сервера Контроль отправки и приёма почты. Настройка прав доступа пользователей к почтовым аккаунтам. Обновление служб сервера. Оптимизация производительности служб сервера. Оптимизация обмена данными со службой SQL - сервера. Оптимизация использования памяти службами.	2	

Самостоятельная работа при изучении тем 2.1., - 2.3. Работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем). Конфигурирование и настройка параметров DHCP Server . Конфигурирование службы и настройка параметров DNS Server.	**50**	

Конфигурирование и настройка параметров информационной системы домена. Конфигурирование настройка параметров групповых политик домена. Конфигурирование и настройка протоколов безопасной передачи информации. Организация статической и динамической маршрутизации, настройка параметров статической и динамической маршрутизации. Организация доступа к сетям Wi-Fi. Настройка параметров Wi-Fi сетей. Организация кэширующего proxy-сервера для доступа в Интернет. Использование трансляции сетевых адресов и прозрачного проксирования для доступа к локальным и глобальным сетям. **Тематика домашних заданий** 1. Изучение аппаратной части. 2. Изучение дополнительных опций конфигурирования web-сервера 3. Изучение запуска, перезапуска и останов сервера под управлением ОС Max ОС. 4. Изучение хостинга нескольких web-узлов. 5. Изучение проблем с производительностью. 6. Изучение безопасности. 7. Изучение организации динамических web-страниц. 8. Изучение проблем с переадресацией адресов. 9. Изучение установки брандмауэра. 10. Изучение порядка прохождения таблиц и цепочек. 11. Изучение трассировки комплексных протоколов. 12. Изучение негативных последствий при сохранение и восстановление больших наборов правил. 13. Изучение основных критериев построения правил. Изучение действий и переходов.		

Учебная практика. **Виды работ:** 1. Установка WEB-сервера 2. Диагностика и обслуживание Web сервера 3. Диагностика и обслуживание файлового сервера 4. Диагностика и обслуживание почтового сервера. 5. Диагностика и обслуживание SQL - сервера 6. Конфигурирование web-сервера. 7. Запуск, перезапуск и останов сервера. 8. Взаимодействие с базами данных. 9. Установка брандмауэра. 10. Сохранение и восстановление больших наборов правил. 11. Обеспечение безопасности. 12. Администрирование серверов и рабочих станций. 13. Организация доступа к локальным сетям и Интернету. 14. Установка и сопровождение сетевых сервисов. 15. Расчёт стоимости сетевого оборудования и программного обеспечения. 16. Сбор данных для анализа использования программно-технических средств компьютерных сетей.	**36**	
Производственная практика (по профилю специальности). **Виды работ:** 1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. 2. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях. 3. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций. 4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. 5. Установка прав доступа и контроль использования сетевых ресурсов. 6. Обеспечение своевременного копирования, архивирования и резервирования данных. 7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. 8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. 9. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 10. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. 11. Осуществление антивирусной защиты локальной вычислительной сети, серверов и	**72**	

рабочих станций				
		Всего	**200**	

2.2.1 Содержание обучения по профессиональному модулю ПМ.01. МДК.02.01 Раздел 2 «Сопровождение модернизации сетевой инфраструктуры»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем.	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ(проект)**	**Объем часов**	**Уровень освоения**
1	**2**	**3**	**4**
МДК.02.01. Раздел 2. Сопровождение модернизации сетевой инфраструктуры		**200**	
		140	
Тема 1.1. Цель и задачи дисциплины.	**Цель и задачи дисциплины.**	**2**	2
Тема 1.2. Характеристики информационных сетей.	**Содержание**	**140**	2
	Основные типы качества обслуживания.		
	Алгоритмы управления очередями ИС		2
	Алгоритмы профилирования и формирования трафика		2
	Предварительное резервирование сетевых ресурсов с помощью протокола RSVP		2
	Периферия компьютерных сетей		2
	Оконечные системы, клиенты и серверы		2

	Ядро компьютерных сетей		2
	Коммутация каналов и коммутация пакетов		2
	Доступ к сети и ее физическая среда		2
	Практические занятия	**60**	
	Практическая работа № 1 «Составления плана качества обслуживания»	2	3
	Практическая работа № 2 «Работа по алгоритму управления очередями ИС»	2	3
	Практическая работа № 3 «Профилирование и формирование трафика»	2	3
	Практическая работа № 4 «Изучение периферии компьютерных сетей»	2	3
	Практическая работа № 5 «Настройка системы клиент-сервер»	2	3
	Практическая работа № 6 «Проектирование ядра компьютерных сетей»	2	3
	Самостоятельная работа.	**50**	
	Доклад: «Поколения информационных сетей»		
	Реферат: «Преимущества телефонных сетей»		
Тема 1.3. **Физический уровень**	**Содержание**		
	Медный кабель , витая пара, Оптическое волокно		2
	Требования при установке кабельной системы.		2
	Практические занятия		
	Практическая работа № 7 «Подключение через медный кабель, через витую пару и оптоволоконный кабель»	2	
	Самостоятельная работа		
	Доклад: «Использование коаксиального кабеля»		

Тема 1.4 Канальный уровень.	**Содержание**		
	Информационная сеть Ethernet, Стандарты Ethernet.		3
	Беспроводные сети		3
	Волоконно-оптические сети.		3
	Технология логической («виртуальной») локальной компьютерной сети (VLAN).		3
	Типовые структуры локальных сетей в корпоративных информационных сетях		3
	Практические занятия		
	Практическая работа № 8 «Настройка информационной сети Ethernet»	2	
	Практическая работа № 9 «Проектирование кольцевой сети с маркером»	2	
	Практическая работа № 10 «Изучение волоконно-оптической сети»	2	
	Практическая работа № 11 «Использование технологии логической («виртуальной») локальной компьютерной сети»	2	
	Самостоятельная работа		
	Реферат: «Топология компьютерных сетей»		
Тема 1.5 Сетевой уровень	**Содержание**		
	Маршрутизация на сетевом уровне	2	3
	Технология TCP/IP	2	3
	Практические занятия		
	Практическая работа № 12 «Настройка маршрутизации»	2	
	Самостоятельная работа		

	Реферат: «Сравнительный анализ концентраторов, коммутаторов и маршрутизаторов»		
	Презентация: «Работа локальной сети с концентратором»		
Тема 1.6 Транспортный уровень	**Содержание**		
	Стандарты транспортного уровня		3
	Присвоение номеров портам приложений		3
	Протокол UDP, Использование протокола **TCP**		3
	Практические занятия		
	Практическая работа № 13 «Присвоение номеров портам приложений»	2	
	Самостоятельная работа		
	Реферат: «Устройство сетевого адаптера»		
Тема 1.7 Технология работы TCP/IP	**Содержание**		
	Драйверы сетевых адаптеров		3
	Установка стека **TCP/IP**		3
	Технология работы при последовательных линиях связи		3
	Виртуальные частные сети VPN		3
	Управление трафиком в ИС		3
	Практические занятия		
	Практическая работа № 14 «Установка драйверов сетевых адаптеров»	2	
	Практическая работа № 15 «Настройка протокола **TCP/IP**»	2	
	Самостоятельная работа		

	Доклад: «Использование технологии Wi-Fi»		
Тема 1.8. Структура Интернета.	**Содержание**		
	Интернет-провайдеры и магистрали Интернета.		3
	Задержки и маршруты в Интернете.		3
	Уровни протоколов и модели их обслуживания.		3
	Многоуровневая структура.		3
	Стек протоколов Интернета.		3
	Практические занятия		
	Практическая работа № 16 «Подключение и настройка сетевого устройства»	2	
	Практическая работа № 17 «Настройка коммуникационного уровня.»	2	
	Самостоятельная работа		
	Реферат: «История развития Интернета В России»		
Тема 1.9 Прикладной уровень.	**Содержание**		
	Протоколы прикладного уровня.		3
	Формат HTTP-сообщения.		3
	Взаимодействие пользователя с сервером.		3
	Область применения HTTP.		3
	Передача файлов по протоколу FTP.		3
	Общие принципы функционирования DNS.		3
	Программирование TCP-сокетов.		3
	Разработка простого web-сервера.		3

	Распределение ресурсов.		3
	Практические занятия		
	Практическая работа № 18 «Передача файлов по протоколу FTP»	2	
	Практическая работа № 19 «Настройка DNS-сервера.»	2	
	Практическая работа № 20 «Изучение алгоритма создания скрипта»	2	
	Самостоятельная работа		
	Реферат: «Способы создания современного сайта»		
Тема 1.10 Транспортный уровень.	**Содержание**		
	Службы транспортного уровня		3
	Взаимодействие между транспортным и сетевым уровнями.		3
	Транспортный уровень в Интернете.		3
	Мультиплексирование и демультиплексирование		3
	Принципы надежной передачи данных.		3
	Протокол TCP.		3
	Контроль перегрузок в TCP. Выравнивание скоростей передачи.		3
	Практические занятия		
	Практическая работа № 21 «Изучение методов мультиплексирования и демультиплексирование»	2	
	Самостоятельная работа		
	Реферат: «Обеспечение надѐжной работы при разных способах подключения»		
Тема 1.11 Сетевой уровень и марш-рутизация	**Содержание**		

	Основы маршрутизации		3
	Алгоритмы маршрутизации		3
	Адресация в протоколе IPv4.		3
	Маршрутизация в Интернете.		3
	Устройство маршрутизатора. Групповая маршрутизация.		3
	Коммутационный блок.		3
	Протокол IPv6.		3
	Практические занятия		
	Практическая работа № 22 «Настройка адресации в протоколе IPv4 и IPv6 »	2	
	Практическая работа № 23 «Разработка модели групповой маршрутизации.»	2	
	Самостоятельная работа		
	Реферат: «Модели сетевого обслуживания»	4	
	Доклад: «Происхождение дейтаграммной службы и службы виртуальных каналов»	4	
	Реферат: «Алгоритм дистанционно-векторной маршрутизации»	4	
	Доклад: «Иерархическая маршрутизация»	4	
Тема 1.12 Локальные сети.	**Содержание**		
	Адресация в локальных сетях и протокол ARP.		3
	Основы технологии Ethernet.		3
	Хабы, мосты, коммутаторы.		3
	Беспроводные каналы связи.		3

	Практические занятия		
	Практическая работа № 24 «Настройка адресации в локальной сети»	2	
	Самостоятельная работа		
	Реферат: «Службы канального уровня»		
	Реферат: «Протоколы коллективного доступа		
Тема 1.13 Безопасность в компьютерных сетях.	**Содержание**		
	Понятие сетевой безопасности. Безопасность на сетевом уровне.		3
	Принципы криптографии. Аутентификация.		3
	Целостность данных. Передача ключей и сертификация.		3
	Управление доступом с помощью брандмауэров.		3
	Безопасность в беспроводных локальных сетях.		3
	Практические занятия		
	Практическая работа № 25 «Использование принципов криптографии»	2	
	Практическая работа № 26 «Настройка аутентификации»	2	
	Самостоятельная работа		
	Реферат: «Генерирование цифровой подписи»		
	Реферат: «Шлюзы прикладного уровня»		
	Реферат: «Безопасная электронная почта»		
Тема 1.14 Сетевое администрирование.	**Содержание**		

	Инфраструктура сетевого администрирования		3
	Архитектура управляющих Интернет-стандартов.		3
	Безопасность и администрирование		3
	Практические занятия		
	Практическая работа № 27 «Создание модели инфраструктуры сетевого администрирования.»	2	
	Самостоятельная работа		
	Доклад: «Структура управляющей информации»		
	Доклад: «Операции и транспортное соответствие протокола »		
Тема 1.15 Операционная система Windows Server.	**Содержание**		
	Установка. Администрирование. Пользователи. Группы. Компьютеры.		3
	Инфраструктура групповой политики. Проверка подлинности		3
	Интеграция DNS с Active Directory Domain Services.		3
	Службы сертификации Active Directory и инфраструктура открытых ключей.		3
	Службы управления правами Active Directory.		3
	Практические занятия		
	Практическая работа № 28 Установка контроллера домена с ядром сервера.	2	
	Практическая работа № 29 Создание настраиваемой консоли MMC и управления ею.	2	
	Практическая работа № 30 Создание и поиск объектов в Active Directory	2	

	Практическая работа № 31 Автоматизация создания учетных записей пользователей.	2	
	Самостоятельная работа		
	Реферат: «Консоль управления Microsoft»		
	Реферат: «Административные инструменты Active Directory»		
	Реферат: «Проектирование структуры подразделений для поддержки делегирования»		
Примерная тематика курсовой работы • Почтовый сервис Яндекса • Организация работы социальной сети «Одноклассники» • Организация работы социальной сети «ВКонтакте» • Виды беспроводной связи в Интернете • Мобильный интернет • Электронный классный журнал • Обслуживание и ремонт сетевого оборудования • Информационно-поисковые системы • Интернет-магазины • История и развитие языка HTML • Создание сайта с помощью конструктора сайтов • Система управления сетевыми сервисами и их распределения • Инструментальные средства поддержки процесса управления требованиями • Инструментальные средства поддержки процесса управления конфигурациями • Управление каталогом услуг с соответствующими классами и определениями услуг • Управление клиентскими данными и SLA. • Управление сетевым реестром и его конфигурация		**30**	

Учебная практика. **Виды работ:** -Настройка, планирование и поддержка сетевой инфраструктуры; -Структурирование и выделение модулей сети; -Разработка сетевых топологий в соответствии с требованиями отказоустойчивости и повышение производительности корпоративной сети; - Выбор принципов проектирования сетей; - Проектирование структурированной кабельной системы (СКС); - Проектирование компьютерной сети, проектирование телефонной сети.	**36**	
Производственная практика (по профилю специальности). **Виды работ:** Знакомство со структурой учреждения, правилами внутреннего распорядка. Инструктаж по охране труда, пожарной безопасности. Организация рабочих мест. Обеспечение защиты трафика протокола IP. Настройка службы удаленного доступа, мониторинга сетевых подключений. Выбор системного программного обеспечения с учетом достоинств новых операционных систем и ввод их в эксплуатацию. Защита сетевого «периметра». Подбор системного программного обеспечения с учетом требований к производительности компьютерной сети. Создание компьютерных учетных записей. Управление учетными записями Управление доступом к ресурсам Доменных служб.	**72**	
Всего:	**140**	

2.2.2 Содержание обучения по профессиональному модулю ПМ.02. МДК02.02, Раздел 1. «Защита от угроз из Интернет»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающегося	Объем часов	Уровень освоения
1	2	3	4
МДК.02.02. Раздел 1. Защита от угроз из Интернет		**420**	
Раздел 1. Защита от угроз из Интернет		**80**	
Введение. **РАЗДЕЛ 1 Введение в безопасность корпоративных сетей**	Информация, ее значимость в современном обществе, возрастание роли информационных ресурсов в жизни и деятельности людей и государства. Определение корпоративной сети. Особенности корпоративных сетей. Актуальность и важность проблемы обеспечения информационной безопасности КС. Угроза безопасности. Способы обеспечения информационной безопасности. Фрагментарный подход, комплексный подход. Принципы построения системы защиты.		1
РАЗДЕЛ 2 Интернет. Основные механизмы сетевого взаимодействия		**17**	
Тема 2.1 Модель OSI и стек протоколов TCP/IP	Введение в сетевой информационный обмен. История создания сети Интернет. Принцип работы сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP	4	1
	Практическое занятие №1 «Утилиты TCP/IP»	2	
Тема 2.2 Службы и сервисы в сети Интернет.	Понятие и структура сервиса. Стандартные и нестандартные сервисы. Принцип работы и функции DNS, WWW, FTP, SMTP. Методы доступа к сервисам**.** Проблемы безопасности при использовании разнородных протоколов. Безопасность IE, Opera, Mozilla.	4	2

	Практическое занятие №2 «Настройка базовых сервисов, входящих в состав операционной системы Windows XP»	4	
	Практическое занятие №3 «Настройка параметров безопасности Web-браузеров IE, Opera, Mozilla»	2	
	Самостоятельная работа: Выполнение домашних заданий по разделу 2 **Тематика внеаудиторной самостоятельно работы** Разработать временную шкалу, на которой отразить основные этапы развития Интернет.	1	
Контрольная работа по разделу 1,2	Подготовка к контрольной работе. Выполнение заданий	2	
РАЗДЕЛ 3 Угрозы информационной безопасности			
Тема 3.1 Анализ угроз сетевой безопасности	Угрозы. Их классификация. Ранжирование угроз по степени деструктивного воздействия. Внутренние и внешние угрозы. Человеческий фактор. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.	4	3
	Практическое занятие №4 «Установка политики IP- безопасности с использованием протокола IPSec»	4	
Тема 3.2 Принципы анализа и построения систем эшелонированной защиты корпоративных сетей	Методология анализа и проектирования системы информационной безопасности. Принцип эшелонированной защиты. Основные компоненты и составные части. Нормативная база анализа защищенности	2	3
	Практическое занятие №5 «Использование программы NetCracker для получения структурно-логических схем локальных сетей»	2	

	Самостоятельная работа: Выполнение домашних заданий по разделу 3 **Тематика внеаудиторной самостоятельно работы** Составить список и проранжировать потенциальные угрозы, возникающие при работе в сети Интернет с домашнего (персонального) компьютера. На структурно-логической схеме локальной сети графически отобразить «точки» применения эшелонированной защиты	2	
Контрольная работа по разделу 3	Подготовка к контрольной работе. Выполнение заданий	2	
РАЗДЕЛ 4 Современные технологии защиты корпоративных сетей			
Тема 4.1 Инструменты мониторинга и анализа сети	Классификация средств мониторинга и анализа. Системы управления сетью, средства управления системой, встроенные системы диагностики и управления, анализаторы протоколов. Значение и необходимость фиксации событий. Журналы. Протоколирование событий ОС Windows. Программы для комплексного журналирования.	2	2
	Практическая работа №6 «Установка и конфигурирование программ мониторинга CommView»	4	
	Практическая работа №7 «Перехват и структурный анализ сетевого трафика с использованием программ CommView, Ethereal»	4	
	Практическая работа №8 «Работа с журналами событий Windows»	4	
Тема 4.2 Системы анализа защищенности	Принципы работы систем анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционных систем. Средства анализа защищенности приложений.	4	3

	Механизмы работы САЗ. Сканеры портов. Сканеры общих ресурсов. Сканеры уязвимостей.		
	Практическое занятие №9 «Анализ уязвимостей локальной системы путем использования сканеров xSpyder, SSS, Microsoft Baseline Security Analyzer»	4	
	Практическое занятие №10 «Сканирование портов с использованием утилиты Nmap»	4	
Тема 4.3 Прикладное ПО системного администратора	Консольные команды. Удаленное администрирование. Проверка работоспособности TCP сервисов.	2	3
	Практическое занятие №11 «Удаленное администрирование посредством программы Remote administrator (Radmin)»	4	
Тема 4.4 Системы обнаружения вторжений	Понятие IDS. Метод сигнатурного анализа, метод обнаружения аномалий. Архитектура системы выявления атак. Классификация СОА. Узловые IDS. Сетевые IDS. Обзор современных IDS.	2	2
	Практическое занятие №12 «Установка и настройка СОА Snort»	4	
Тема 4.5 Основные принципы построения и функционирования межсетевых экранов (МЭ)	Общие сведения о межсетевых экранах. Перехват пакетов. Анализ пакетов. Обработка ситуации. Интерфейсы межсетевых экранов. Дополнительные функции. Многофункциональные решения на базе МЭ. Программные и аппаратные МЭ. Персональные МЭ. Политика работы МЭ. Проблемы безопасности МЭ	4	2
	Практическое занятие №13 «Настройка стандартной конфигурации Kerio Winroute Firewall с использованием мастера и шаблонов»	2	
	Практическое занятие №14 «Настройка Kerio Winroute Firewall для организации контроля доступа и трафика в корпоративной сети»	2	

Тема 4.6 Виртуальные частные сети	Принцип работы и классификация VPN. Протоколы построения виртуальных частных сетей (VPN) и алгоритмы их работы Сравнительный обзор российского рынка VPN. Типовые решения по защите корпоративной сети на основе применения VPN. Построение защищенных сетей на канальном (протоколы PPTP, L2F, L2TP), сетевом (протоколы IPSec, IPv6) и сеансовом (протоколы SSL, SOCKS) уровнях.	4	2
	Практическое занятие №15 «Создание VPN туннеля с использованием Kerio VPN Client»	2	
Тема 4.7 Технологии антивирусной защиты	Понятие и классификация вирусов. Жизненный цикл вирусов. Другие виды вредоносного ПО. Каналы распространения вредоносных программ. Обзор методов антивирусной защиты. Сигнатуры. Виды антивирусного ПО. Корпоративные системы антивирусной зашиты.	4	3
	Практическое занятие №16 «Установка и настройка Kaspersky Internet Security»	2	
	Практическое занятие № 17 «Настройка Symantec Antivirus CE для защиты распределенной вычислительной сети».	2	
	Самостоятельная работа: **Тематика внеаудиторной самостоятельно работы** Перехватить сетевой трафик при работе в сети Интернет с домашнего (персонального) компьютера.	1	
Контрольная работа по разделу 4	Подготовка к контрольной работе. Выполнение заданий	2	
	Всего:	**100**	

2.2.3 Содержание обучения по профессиональному модулю ПМ.02. МДК.02.02, Раздел 2. «Основы компьютерной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающегося	Объем часов	Уровень освоения
1	2	3	4
МДК.02.02, Раздел 2. «Основы компьютерной безопасности»		**420** **100**	
Введение. РАЗДЕЛ 1 Определение предмета “Основы компьютерной безопасности”			
Тема 1.1 Безопасность компьютерных систем. Основные понятия и определения	Цели и задачи учебной дисциплины. Связь дисциплины с другими дисциплинами учебного курса. Учебная и техническая литература. Понятие и положения компьютерной безопасности. История и предпосылки возникновения проблемы, актуальность и важность.	**2**	1
Тема 1.2 Анализ угроз безопасности компьютерных систем	Понятие, системная классификация и общий анализ угроз безопасности информации.	**2**	2
Тема 1.3 Состояние и прогноз развития компьютерной безопасности в России и за рубежом	Состояние и прогноз развития компьютерной безопасности за рубежом. Состояние компьютерной безопасности в России: - особенности экономического развития России - показатели экономической безопасности и ее влияние на компьютерную безопасность компьютерной безопасности России. Основные угрозы безопасности России в информационной сфере.	**4**	1
Тема 1.4 Методы обеспечения компьютерной безопасности	Наиболее важные аспекты проблемы безопасности компьютерных технологий: - защищенные ОС и сертифицированные ФСТЭК средства защиты от НСД, - криптографические методы защиты и антивирусная защита; - защита программного обеспечения от несанкционированного копирования и корпоративных сетей от угроз из Internet;	**4**	2

	защита цепей питания и каналов передачи данных.		
Тема 1.5 Модель угроз и принципы обеспечения безопасности ПО компьютерных систем	Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность. Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире	**2**	2
Тема 1.6. Защищенные операционные системы	Классификация и группы угроз операционных систем (ОС). Понятие и компоненты защищенной ОС. Подходы к построению защищенных ОС. Подсистема защиты ОС.	**4**	2
Тема 1.7 Защита в ОС Unix, Windows	Средства и механизмы безопасности в ОС Unix, Windows.	**4**	3
	Практическое занятие №1: «Настройка механизмов безопасности ОС Windows»	**10**	
Контрольная работа по разделу 1	Подготовка к контрольной работе. Выполнение заданий	**2**	
РАЗДЕЛ 2. Методология построения защищенных компьютерных систем		**47**	
Тема 2.1 Требования к построению защищенных автоматизированных систем	Классификация требований к системам защиты. Формализованные требования к защите информации от НСД- система нормативных документов в России и за рубежом. Общие подходы к построению систем защиты компьютерной информации	**2**	2
Тема 2.2 Отечественные и зарубежные стандарты в области компьютерной безопасности	Зарубежные стандарты в области компьютерной безопасности: - органы, отвечающие за компьютерную безопасность в США и Европе - система нормативных документов США в области компьютерной безопасности. Российские стандарты в области компьютерной безопасности: - органы, отвечающие за компьютерную безопасность в России - обзор руководящих документов ФСТЭК в области компьютерной безопасности.	**4**	3
Тема 2.3 Сертифицированные ФСТЭК средства защиты от НСД	Основные принципы защиты информации. Назначение, возможности и классификация систем защиты компьютеров от НСД. Основные производители и их продукция	**2**	3
Тема 2.4 Система защиты от НСД Secret Net	Основные функциональные возможности и характеристики. Состав и структура системы	**2,5**	3

	Практическое занятие №2: «Введение в систему защиты от НСД Secret Net. Установка, обновление, удаление системы защиты от НСД Secret Net»	**2**	
	Практическое занятие №3: «Настройка системы защиты от НСД Secret Net. Общие параметры системы»	**2**	
	Практическое занятие №4: «Настройка прав доступа администратора и пользователей системы защиты от НСД Secret Net»	**4**	
	Практическое занятие №5: «Управление доступам к ресурсам в системе защиты от НСД Secret Net»	**2**	
	Практическое занятие №6: «Порядок работы с системным журналом системы защиты от НСД Secret Net»	**2**	
Контрольная работа по теме 2.4	Подготовка к контрольной работе. Выполнение заданий	**2**	
Тема 2.5 Система защиты от НСД Dallas lock	Основные функциональные возможности и характеристики. Состав и структура системы	**2,5**	3
	Практическое занятие №7: «Введение в систему защиты от НСД Dallas lock. Установка, обновление, удаление системы защиты от НСД Dallas lock»	**2**	
	Практическое занятие №8: «Настройка прав доступа администратора и пользователей системы защиты от НСД Dallas lock»	**2**	
	Практическое занятие №9: «Дополнительная настройка системы Dallas Lock»	**2**	
	Практическое занятие №10: «Настройка журналов системы»	**2**	
Контрольная работа по теме 2.5	Подготовка к контрольной работе. Выполнение заданий	**2**	
Контрольная работа по разделу 2	Подготовка к контрольной работе. Выполнение заданий	**2**	
Раздел 3. Криптографические методы защиты информации			
Тема 3.1 Введение в криптографическую защиту информации	Введение в криптографическую защиту информации. Классификация криптоалгоритмов: - симметричные криптоалгоритмы - асимметричные криптоалгоритмы	**4**	
	Практическое занятие № 11: «Работа с криптографической программой PGP (Pretty Good Privacy)»	**2**	

Раздел 4. Технология антивирусной защиты			
Тема 4.1 Вирусы	Понятие и классификация вирусов. Жизненный цикл вирусов. Другие виды вредоносного ПО. Каналы распространения вредоносных программ.	**2**	2
Тема 4.2 Антивирусное программное обеспечение	Обзор методов антивирусной защиты. Сигнатуры. Виды антивирусного ПО	**2**	3
	Практическое занятие № 12. «Установка и настройка Kaspersky Internet Security»	**2**	
Контрольная работа по разделу 3, 4	Подготовка к контрольной работе. Выполнение заданий	**2**	
Раздел 5. Технологии сетевой защиты			
Тема 5.1 Технологии информационной защиты сетей	Проблемы безопасности современных сетей. Обеспечение безопасности сетей: криптографическая защита данных, технологии межсетевых экранов, технологии виртуальных защищенных каналов и сетей VPN, технологии обнаружения вторжений	**1**	2
Тема 5.2 Межсетевые эраны	Назначение и основные возможности межсетевых экранов. Программные и аппаратные МЭ. Персональные МЭ. Политика работы МЭ. Проблемы безопасности МЭ.	**2**	2
Тема 5.3 Виртуальные частные сети	Принцип работы и классификация VPN. Протоколы построения виртуальных частных сетей (VPN) и алгоритмы их работы Типовые решения по защите корпоративной сети на основе применения VPN.	**2**	2
Тема 5.4 Системы обнаружения вторжений	Понятие системы обнаружения вторжений (IDS). Метод сигнатурного анализа, метод обнаружения аномалий. Архитектура системы выявления атак. Классификация IDS	**2**	2
Тема 5.5. Системы анализа защищенности	Понятие системы анализа защищенности (САЗ). Классификация САЗ. Принципы работы систем анализа защищенности. работы САЗ.	**2**	3
	Практическое занятие № 13: «Анализ защищенности информационной системы на основе выявления уязвимостей и обнаружения вторжений»	**2**	
Контрольная работа по разделу 5	Подготовка к контрольной работе. Выполнение заданий	**2**	
	Всего:	**120**	

2.2.4 Содержание обучения по профессиональному модулю ПМ.02. МДК.02.02, Раздел 3. «Защита информации в Компьютерных сетях»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающегося	Объем часов	Уровень освоения
1	2	3	4
МДК.02.02, Раздел 3. «Защита информации в Компьютерных сетях»		**420** **100**	
Введение. РАЗДЕЛ 1 Определение предмета “Защита информации в КС”		**70**	
Тема 1.1 Анализ угроз безопасности компьютерных систем	Цели и задачи учебной дисциплины. Связь дисциплины с другими дисциплинами учебного курса. Учебная и техническая литература. Понятие и положения компьютерной безопасности. История и предпосылки возникновения проблемы, актуальность и важность. Понятие, системная классификация и общий анализ угроз безопасности информации	2	1
Тема 1.1 Обнаружение компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий.	2	2
Тема 1.2 Состояние и прогноз развития компьютерной безопасности в России и за рубежом	Состояние и прогноз развития компьютерной безопасности за рубежом. Состояние компьютерной безопасности в России: - особенности экономического развития России - показатели экономической безопасности и ее влияние на компьютерную безопасность компьютерной безопасности России. Основные угрозы безопасности России в информационной сфере.	2	1
Тема 1.3 Механизмы типовых атак	Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий.	2	3

Тема 1.4 Классификация систем обнаружения атак (СОА).	Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак	4	3
Тема 1.5 Архитектура СОА	Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.	4	3
Тема 1.6 Технология межсетевого экранирования	Стратегии и средства межсетевого экранирования. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Обзор документов RFC, регламентирующих использование межсетевых экранов. Типы межсетевых экранов. Схемы межсетевого экранирования.	2	3
Тема 1.7 Фильтрация пакетов	Критерии и правила фильтрации. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Организация узлов для отвлечения внимания злоумышленника. Особенности фильтрации различных типов трафика. Пакетный фильтр на базе ОС Windows 2000-XP. Служба RRAS. Программа управления службой RRAS	4	3
Тема 1.8 Шлюзы прикладного уровня.	Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации. Контроль HTTP-трафика и электронной почты. Написание правил фильтрации, возможности по анализу содержимого.	4	3
Тема 1.8 Организация виртуальных частных сетей	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Установка и настройка VPN. Анализ защищенности передаваемой информации.	4	3
Тема 1.9 Защита данных на сетевом уровне.	Протокол SKIP. Протокол IPSec. Организация VPN средствами СЗИ «VipNet». Использование протокола IPSec для защиты сетей. Шифрование трафика с использованием протокола IPSec. Настройка политики межсетевого экранирования с использованием протокола IPSec.	4	3
Тема 1.10 Организация VPN средствами СЗИ «StrongNet»	Организация VPN средствами СЗИ «StrongNet». Описание системы. Генерация и спространение ключевой информации. Настройка СЗИ «StrongNet». Установка защищенного соединения.	4	3

Тема 1.11 Защита на транспортном уровне.	Организация VPN средствами протокола SSL в Windows Server 2008. Генерация сертификата открытого ключа для web-сервера. Настройка SSL-соединения.	4	3
Тема 1.12 Организация VPN прикладного уровня	Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Защищенный обмен электронной почтой.	4	3
Тема 1.13 Технологии защищенной обработки информации	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2008. Настройка сервера MSTS. Настройка протокола RDP.	4	3
Тема 1.14 Службы каталогов.	Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory	4	3
Тема 1.15 Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности.	4	3
Тема 1.16 Структура информационно - телекоммуникационных сетей	Определение структуры информационно телекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации.	2	3
Тема 1.17 Сетевой мониторинг	Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети.	2	3
Тема 1.18 Уязвимости в программном обеспечении узлов компьютерной сети.	Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений.	4	3
Тема 1.19 Структура и функции комплексных экспертных систем аудита	Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта	2	3

	информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.		
Темы практических работ		**50**	
	Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute		
	Защита сетевого трафика с использованием протокола IPSec в Windows NT 5.0. Организация VPN средствами протокола PPTP		
	Применение специализированных средств организации VPN на примере «VipNet» и «StrongNET»		
	Применение COA Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании»		
	Применение технологии терминального доступа		
	Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз		
	Всего:	**100**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

3. *УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ*

3.1 Материально-техническое обеспечение

Требования к минимальному материально-техническому обеспечению ПМ.02, Раздел 1 «Организация сетевого администрирования».

Реализация программы модуля предполагает наличие учебного кабинета Математических принципов построения компьютерных сетей

Оборудование учебного кабинета:

1. -автоматизированные рабочие места по количеству обучающихся;
2. -автоматизированное рабочее место преподавателя;
3. -специализированная мебель;
4. -комплект нормативных документов;
5. -комплект учебно-методической литературы.
6. *Технические средства обучения:*
7. -проектор;
8. -экран;
9. -сканер;
10. -принтер;
11. -программное обеспечение общего и профессионального назначения.

3.2 Информационное обеспечение обучения

Основные источники:

1. Компьютерные сети [Текст] : учебное пособие / Е. О. Новожилов. - М : Издательский центр "Академия", 2013.
2. Баранчиков А.И. Организация сетевого администрирования : учебник М : Издательский центр "Академия", 2016

Дополнительные источники:

1. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд., СПб: Питер, 2015г.
2. Ватаманюк А. Создание, обслуживание и администрирование сетей на 100%, СПб: Питер, 2010г.
3. Колисниченко Д. Linux. От новичка к профессионалу, СПб: БХВ-Петербург, 2011г.
4. Станек Уильям Р. Командная строка Microsoft Windows. Справочник администратора, СПб: БХВ-Петербург, 2009г.
5. Станек Уильям Р. Windows PowerShell 2.0. Справочник администратора, СПб: БХВ-Петербург, 2010г.
6. Кришнамурти Б., Рексфорд Дж. Web-протоколы. Теория и практика, М: Бином 2010г.
7. Скотт Хокинс , Администрирование web-сервера APACHE и руководство по электронной коммерции., Издательский дом «Вильями», Москва, Санкт-Петербург, Киев, 2010 г.
8. http://www.linuxshare.ru/docs/security/iptables/iptables-tutorial.html

Интернет-ресурсы и электронно-библиотечные системы:

1. www.elibrary.ru — научная электронная библиотека (НЭБ).
2. http://lib.uni-dubna.ru/biblweb/ - сайт библиотеки университета «Дубна» с доступом к электронному каталогу и другим библиотечно-информационным ресурсам
3. http://lib.uni-dubna.ru/biblweb/search/resources.asp?sid=18 - специализированный раздел сайта библиотеки с доступом к электронным ресурсам, предоставляемых на основе лицензионных соглашений, заключенных между организациями - держателями ресурсов и университетом «Дубна»

Требования к минимальному материально-техническому обеспечению ПМ.02, Раздел 2 «Сопровождение модернизации сетевой инфраструктуры».

Реализация профессионального модуля предполагает наличие учебных кабинетов:
кабинет математического аппарата и построения компьютерных сетей,
лаборатория эксплуатации объектов сетевой инфраструктуры.
Оборудование учебного кабинета и рабочих мест кабинета посадочные места по количеству обучающихся; рабочее место преподавателя; сервер; сетевое оборудование: концентратор на 16 портов, коммутатор на 12 портов, сканер, мультимедийный комплекс для группового пользования, интерактивная доска, принтеры, комплект инструкционно-технологических карт.

Средства обучения:

- Комплект бланочной документации, АРМ (автоматизированное рабочее место), серверные операционные системы (Microsoft Windows Server, Microsoft Small Business Server), почтовые серверы (Microsoft Exchange, MDaemon и др.), специализированное серверное лицензионное программное обеспечение различных разработчиков (тренажеры, модели, макеты, оборудование, технические средства, в т.ч. аудиовизуальные, компьютерные и телекоммуникационные и т.п.) комплект справочной, нормативной, технической документации;
- комплект учебно-методической документации.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Попов И.И., Максимов Н.В. Компьютерные сети: Учебное пособие для студентов учреждений среднего профессионального образования. - М.: ФОРУМ:ИНФРА-М, 2015.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - СПб.: Питер, 2014.
3. Вендров А.М. Проектирование программного обеспечения экономических информационных систем: учебник - 2-е изд., перераб. и доп. М.: Финансы и статистика, 2014.
4. Мейер Б. Объектно-ориентированное конструирование программных систем: пер. с англ. М.: Русская редакция, 2012.
4. Костров Б.В. Технологии локальных сетей и др.: Учебное пособие. Теле-коммуникационные системы и вычислительные сети: Основы сетей передачи данных; Технология "клиент - сервер", ТехБук, 2012г.

Дополнительные источники:

1. Ю.А. Головин, А.А. Суконщиков/ Информационные сети, Москва, Академия, 2011
2. В. Олифер, Н. Олифер/ Основы компьютерных сетей, Питер, 2011
3. В.М. Вишневский. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2012. – 512 с.
4. С.Д. Пароджанов. Методология создания корпоративных ИС
5. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных: Курс лекций. Интернет-Университет информационных технологий -ИНТУИТ.РУ, 2013
6. Дуглас Э. Камер. Сети ТСРЛР. - М.: Вильяме, 2013. - Т. 1: Принципы,

протоколы и структура.
7. Таненбаум Э. Компьютерные сети. - Питер, 2012.
8. Михаил Гук. Аппаратные средства локальных сетей: Энциклопедия. - СПб.: Питер, 2010.

Интернет-ресурсы:

1. www.edu.ru/modules.php. - Каталог образовательных Интернет-ресурсов: учебно-методические пособия.
2. http://www.viomedia.ru/ Интеграция сетевой инфраструктуры и обеспечение информационной безопасности
3. http://www.uchenik.ru/ статьи по сетевым технологиям
4. http://www.bookshunt.ru/ книги по сетевым технологиям
5. http://www.labirint.ru/ Книги для профессионалов

Требования к минимальному материально-техническому обеспечению ПМ.02, Раздел 1 «Защита от угроз из Интернета».

Реализация раздела междисциплинарного курса требует наличия учебного кабинета и компьютерного класса.

Оборудование учебного кабинета:

1. посадочные места по количеству обучающихся;
2. рабочее место преподавателя
3. доска

Технические средства обучения:

1. компьютер с лицензионным программным обеспечением;
2. проектор;

Оборудование компьютерного класса и рабочих мест:

1. посадочные места по количеству обучающихся;
2. компьютеры с лицензионным программным обеспечением, объединенные в локальную вычислительную сеть;

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПбГУ ИТМО, 2014.- 161 с.
2. Прохода А.Н. Обеспечение интернет- безопасности. Практикум: Учебное пособие для вузов.- М.: Горячая линия- телеком, 2017.- 180 с.: ил.
3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. Шаньгин В. Ф. - М.: ДМК Пресс, 2010.- 544 с.: ил.
4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2014.- 592 с.: ил.
5. Щербаков А. Ю. Современная Компьютерная Безопасность. Теоретические Основы. Практические Аспекты. – цифровая книга, 2015.- 352 с.: ил.

Дополнительные источники:

1. Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А. С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. ПРАКТИЧЕСКИЙ КУРС: учебное пособие / А. Н.

Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург : УГТУ-УПИ, 2015. 248 с.
2. Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2014. – 225 с.
3. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2014. — 85 с.
4. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2015. — 256 с.

Требования к минимальному материально-техническому обеспечению ПМ.02, Раздел 2 «Основы компьютерной безопасности».

Требования к минимальному материально-техническому обеспечению

Реализация раздела междисциплинарного курса требует наличия учебного кабинета и компьютерного класса.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя
- доска

Технические средства обучения:

- компьютер с лицензионным программным обеспечением
- проектор

Оборудование компьютерного класса и рабочих мест:

- посадочные места по количеству обучающихся;
- компьютер с лицензионным программным обеспечением.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

6. А. А. Грушо, Э. А. Применко, Е. Е. Тимонина Теоретические основы компьютерной безопасности. - М.: Академия, 2009.- 272 с.: ил.
7. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. Шаньгин В. Ф. - М.: ДМК Пресс, 2010.- 544 с.: ил.
8. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012.- 592 с.: ил.
9. Щербаков А. Ю. Современная Компьютерная Безопасность. Теоретические Основы. Практические Аспекты. – цифровая книга, 2009.- 352 с.: ил.

Дополнительные источники:

5. Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А. С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. ПРАКТИЧЕСКИЙ КУРС: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург : УГТУ-УПИ, 2008. 248 с.

Требования к минимальному материально-техническому обеспечению ПМ.02, Раздел 3 «Защита информации в Компьютерных сетях».

Материально-техническое обеспечение дисциплины

Практические занятия должны выполняться в специализированных компьютерных классах, имеющих в составе:
• персональные ЭВМ, объединенные в локальную вычислительную сеть Ethernet. Минимальные требования к персональным компьютерам: платформа IA-32, тактовая частота центрального процессора не ниже 2 ГГц, оперативная память объемом не менее 512 Мбайт, жесткие магнитные диски с интерфейсом Serial ATA и емкостью не менее 300 Мбайт;
• персональный компьютер преподавателя с мультимедиа-проектором и экраном — 1 комплект;
• операционные системы семейства MS Windows NT 5.0 (лицензии по числу рабочих мест);
• программное обеспечение организации виртуальных сетей VMware Workstation (лицензии по числу рабочих мест);
• СЗИ VPN «VipNET»
• СЗИ VPN «StrongNET»
• СКЗИ КриптоПро CSP

Основные источники:

1. Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А. С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ. ПРАКТИЧЕСКИЙ КУРС: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург : УГТУ-УПИ, 2015. 248 с.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2015. — 256 с.
3. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2015. — 256 с.

Дополнительные источники:

1. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.
2. Щербаков А. Ю. Современная Компьютерная Безопасность. Теоретические Основы. Практические Аспекты. – цифровая книга, 2015.- 352 с.: ил.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02. Раздел 1, «Организация сетевого администрирования»

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.	•Обеспечивать бесперебойное функционирование вычислительной сети в соответствии с техническими условиями и нормативами обслуживания •Проводить необходимые тестовые проверки и профилактические осмотры •Осуществлять мониторинг использования вычислительной сети •Фиксировать и анализировать сбои в работе серверного и сетевого оборудования •Обеспечивать своевременное выполнение профилактических работ •Своевременно выполнять мелкий ремонт оборудования •Фиксировать необходимость внеочередного обслуживания программно технических средств •Соблюдать нормы затрат материальных ресурсов и времени •• Вести техническую и отчетную документацию	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на практических, учебной и производственной практики.
ПК 2.2. Администрировать сетевые ресурсы в информационных системах	•Администрировать размещённые сетевые ресурсы •Поддерживать актуальность сетевых ресурсов •Организовывать доступ к локальным и глобальным сетям, в том числе, в сети Интернет •Обеспечивать обмен информацией с другими организациями с использованием электронной почты •Контролировать использование сети Интернет и электронной почты •Сопровождать почтовую систему •Применять новые технологии системного администрирования	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на практических, учебной и производственной практики.

ПК 2.3. Обеспечить сбор данных для анализа использования и функционирования программнотехнических средств компьютерных сетей.	•Обеспечивать наличие программно-технических средств сбора данных для анализа показателей использования и функционирования компьютерной сети •Осуществлять мониторинг производительности сервера •Протоколировать системные и сетевые события •Протоколировать события доступа к ресурсам •Применять нормативно-техническую документацию в области информационных технологий	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы при выполнении работ на практических, учебной и производственной практики.
ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.	•Совместно планировать развитие программно-технической базы организации •Обосновывать предложения по реализации стратегии в области информационных технологий •Определять влияние системного администрирования на процессы других подразделений •Подготавливать совместно с другими подразделениями технические совещания •Применять отечественный и зарубежный опыт использования программно-технических средств •Участвовать в научных конференциях, семинарах.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы на практических занятиях (при выполнении и защите лабораторных работ, при решении ситуационных задач, при участии в деловых играх, при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02. Раздел 1, «Защита от угроз из Интернет»

Контроль и оценка результатов освоения раздела междисциплинарного курса осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	2
Знать:	
терминологию в области безопасности корпоративных сетей;	Практические занятия. Контрольные работы. Домашняя работа
методологию построения безопасных корпоративных сетей;	Практические занятия. Контрольные работы. Домашняя работа
современные сетевые технологии и сервисы;	Практические занятия. Контрольные

	работы. Домашняя работа
Уметь:	
анализировать угрозы безопасности корпоративной сети;	Практические занятия
разрабатывать и реализовывать предложения по созданию системы защиты для конкретных корпоративных сетей;	Практические занятия

4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02. Раздел 2, «Основы компьютерной безопасности».**

Контроль и оценка результатов освоения раздела междисциплинарного курса осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	2
Знать:	
наиболее важные аспекты проблем безопасности компьютерных технологий;	Практические занятия. Контрольные работы. Домашняя работа
основные средства и методы защиты компьютерной информации;	Практические занятия. Контрольные работы. Домашняя работа
основные пакеты прикладных программ по защите информации;	Практические занятия. Контрольные работы. Домашняя работа
Уметь:	
устанавливать, обслуживать, применять средства защиты информации от НСД;	Практические занятия
обеспечивать защиту информации и управление доступом к информационным ресурсам в информационных системах.	Практические занятия

4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02. Раздел 3, «Защита информации в компьютерных сетях».**

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	***Формы и методы контроля и оценки***
Понимать сущность и социальную значимость своей будущей	– демонстрация интереса к будущей профессии; – использование современных методов и	*Интерпретация результатов*

профессии, проявлять к ней устойчивый интерес	средств информационных технологий при разработке информационных систем.	*наблюдений за деятельностью обучающегося в процессе освоения образовательной программы*
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	– применение методов ИТ при решении профессиональных задач; – выдвижение нестандартных идей при решении профессиональных задач. – оценка эффективности и качества выполнения;	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	– решать стандартных и нестандартных профессиональных задач в области разработки технологических процессов изготовления деталей машин; – Владение методами влияния человека-оператора на функционирование информационных систем.	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	– эффективный поиск необходимой информации; – использование различных источников, включая электронные; – использование методов и средств организации, проектирования, разработки и применения систем, предназначенных для обработки информации.	
Использовать информационно-коммуникационные технологии в профессиональной деятельности	– использование методов и средств информационных и телекоммуникационных технологий; – владение методами анализа информационных ресурсов.	
Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями	– взаимодействие с обучающимися и преподавателями в ходе обучения – использование промышленных стандартизированных решений, опирающихся на современные информационно-коммуникационные технологии. – владение методами анализа проектных решений.	
Брать на себя ответственность за	– самоанализ и коррекция результатов собственной работы;	

работу членов команды (подчиненных), за результат выполнения заданий	– использование моделей администрирования сети и способов обеспечения безопасности информационных систем.	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	– организация самостоятельных занятий при изучении профессионального модуля; – использование методов по созданию экспертных систем и автоматизированных обучающих систем; – использование основных средств для определения запросов и процедурных языков	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	– анализ инноваций в области разработки программного обеспечения; – использование структуры информационных систем, методов и средств информационных и телекоммуникационных технологий.	
Обеспечивать безопасные условия труда в профессиональной деятельности	– соблюдение техники безопасности;	