Приложение III.31
к образовательной программе
по специальности 09.02.01
Компьютерные системы и комплексы

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА И КОМПЬЮТЕРНЫХ СЕТЕЙ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6FA44C50384686A8E7BD5E27735179BC
Владелец: Ефремова Вероника Васильевна
Действителен: с 14.06.2022 до 07.09.2023

Рабочая программа разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, утверждённого приказом Министерства образования и науки РФ от 28.07.2014 г. № 849 (зарегистрировано в Министерстве юстиции РФ 21.08.2014 г., № 33748)

Рабочая программа рассмотрена
на заседании ЦК ИТ АиЭС
протокол № 11 от «09» июня 2022 г.
Председатель ЦК
_____ Т.А. Петрова

УТВЕРЖДАЮ
Заместитель директора по УМР
_____ Т.Б. Балобанова
«09» июня 2022 г.

Рабочую программу разработал:
преподаватель высшей квалификационной категории, инженер-системотехник, преподаватель среднего профессионального образования и ДПО
_____ М.И. Петрова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА И КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Место дисциплины в структуре образовательной программы: учебная дисциплина ОП.11 Информационная безопасность персонального компьютера и компьютерных сетей входит в профессиональный учебный цикл ППССЗ как общепрофессиональная дисциплина вариативной части.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК, ДК	*Умения*	*Знания*	*Практический опыт*
ОК 1 – 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– проводить анализ и оценку уязвимостей компьютерной системы; – применять меры информационной безопасности процедурного уровня; – осуществлять защиту информации от несанкционированного доступа; – настраивать безопасность почтового клиента; – настраивать параметры аутентификации пользователей; – осуществлять регистрацию и аудит информационной безопасности; – настраивать системы разграничения доступа; – применять криптографические методы и средства зашиты информации; – использовать средства антивирусной защиты; – использовать стандарты и спецификации информационной безопасности.	– понятие и составляющие информационной безопасности; – виды угроз информации и методы защиты от них; – законы, стандарты и спецификации информационной безопасности; – меры процедурного уровня информационной безопасности; – меры программно-технического уровня информационной безопасности; – методы защиты информации от несанкционированного доступа; – способы разграничения полномочий и доступа к объектам; – осуществление регистрации и аудита в компьютерной системе; – проведение оценки рисков компьютерной системы; – применение средств антивирусной защиты.	– применения средств и методов защиты информации; – выбора, установки и настройки средств защиты информации.

Код	Наименование общих компетенций
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Код	Наименование профессиональных компетенций
ПК 2.3	Осуществлять установку и конфигурирование персональных компьютеров и подключение периферийных устройств.
ПК 3.3	Принимать участие в отладке и технических испытаниях компьютерных систем и комплексов, инсталляции, конфигурировании программного обеспечения.

Код	Наименование дополнительных компетенций
ДК 11.1	Применять программно-аппаратные средства обеспечения информационной безопасности в компьютерных системах
ДК 11.2	Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем учебной дисциплины	**120**
в том числе:	
теоретическое обучение	48
практические занятия	24
Самостоятельная работа (в том числе консультации)	48
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины ОП.11 Информационная безопасность персонального компьютера и компьютерных сетей

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Концепция и политики безопасности в сетях		**26**	
Тема 1.1. Концепция информационной безопасности	**Содержание учебного материала**	4	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1.Основные понятия информационной безопасности.		
	2.Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.		
	3.Комплексный подход к защите информации.		
	4.Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический.		
	5.Требования к комплексным системам защиты информации		
	Самостоятельная работа 1. Проанализировать профессионально – значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности	4	
Тема 1.2. Нормативно-правовые основы обеспечения информационной безопасности персонального компьютера и компьютерных сетей	**Содержание учебного материала**	4	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1. Статьи Конституции Российской Федерации в области информационной безопасности. Статьи Гражданского и Уголовного кодексов Российской Федерации в области информационной безопасности.		
	2. Закон «Об информации, информатизации и защите информации».		
	3.Отдельные законы и нормативные акты Российской		

	Федерации в области информационной безопасности		
	4.Оценочные стандарты и технические спецификации. в области защиты информации		
	Самостоятельная работа 2. Составить перечень основный понятий и определений, используемых в нормативно – правовых документах	4	
Тема 1.3. Угрозы информационной безопасности в компьютерных системах и сетях	**Содержание учебного материала**	2	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1.Понятие угрозы информационной безопасности в компьютерных системах и сетях.		
	2.Классификация и анализ угроз информационной безопасности в компьютерных системах и сетях.		
	3.Случайные угрозы информационной безопасности.		
	4.Преднамеренные угрозы информационной безопасности.		
	5.Меры защиты от угроз в компьютерных системах и сетях.		
	Самостоятельная работа 3. Для выбранного объекта защиты информации провести анализ защищенности объекта.	8	
Раздел 2. Методы и средства обеспечения информационной безопасности в компьютерных системах и сетях		**60**	
Тема 2.1. Защита информации от несанкционированного доступа	**Содержание учебного материала**	8	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1. Характеристика средств защиты информации в компьютерных системах и сетях от несанкционированного доступа.		
	2. Идентификация и аутентификация пользователей.		
	3. Управление доступом.		
	4. Протоколирование и аудит.		
	Практическое занятие 1. Настройка параметров аутентификации Windows 7	2	
	Практическое занятие 2. Управление шаблонами безопасности в Windows 7.	2	
	Практическое занятие 3. Назначение прав пользователей при произвольном управлении доступом в Windows 7.	2	

	Практическое занятие 4. Настройка параметров регистрации и аудита в Windows 7.	2	
Тема 2.2. Криптографические методы защиты информации	**Содержание учебного материала**	8	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1.Основные понятия криптографии. Классификация криптографических средств.		
	2.Симметричные криптосистемы.		
	3.Ассиметричные криптосистемы.		
	4.Электронная цифровая подпись и ее применение для контроля целостности программ и данных.		
	5.Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены		
	6.Метод аналитических преобразований.		
	7. Понятие криптоатаки. Классификация криптоатак.		
	Практическое занятие 5. Шифрующая файловая система EFS и управление сертификатами в Windows.	2	
	Практическое занятие 6. Методы криптографического преобразования данных.	2	
	Самостоятельная работа 4. Шифрование и дешифрование текста методом перестановок	4	
	Самостоятельная работа 5. Шифрование и дешифрование текста методом замены	4	
	Самостоятельная работа 6. Рассмотреть особенности и принципы работы стандартных и специализированных программных средств шифрования.	8	
Тема 2.3. Компьютерные вирусы и средства антивирусной защиты	**Содержание учебного материала**	4	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1.Общие сведения о компьютерных вирусах.		
	2.Классификация компьютерных вирусов.		
	3.Методы и средства защиты от компьютерных вирусов.		
	4.Антивирусные программные комплексы.		
	Практические занятия №7. Антивирусные программные комплексы	2	
	Практические занятия №8.Восстановление зараженных	2	

	файлов. Профилактика проникновения «троянских программ».		
	Самостоятельная работа №7. Разработать контролирующий, диагностический или демонстрационный материал по теме	2	
	Самостоятельная работа №8. Построить схему системы антивирусной защиты корпоративной сети (на примере).	6	
Раздел 3. Базовые технологии сетевой безопасности		**34**	
Тема 3.1. Выявление сетевых атак путем анализа трафика	**Содержание учебного материала**	6	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1. Этапы сетевой атаки. Исследование сетевой топологии. Обнаружение доступных сетевых служб.		
	2. Виды анализаторов трафика. Методика работы с сетевыми анализаторами с целью определения структуры сетевых пакетов на примере программы Ethereal.		
	3. Выявление уязвимых мест атакуемой системы. Выявление атаки на протокол SMB.		
	4. Системы обнаружения атак. Сетевые решения.		
	Практическое занятие 9. Изучение интерфейса программы анализатора трафика	2	
	Практическое занятие 10. Фильтрация пакетов и захват трафика.	2	
Тема 3.2. Защита компьютерной сети с использованием межсетевых экранов	**Содержание учебного материала**	4	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1. Понятие межсетевого экрана. Компоненты межсетевого экрана. Архитектура межсетевого экрана. Политика межсетевого экранирования.		
	2. Функции межсетевого экрана. Применение технологии трансляции сетевых адресов		
	3. Виды межсетевых экранов.		
	4. Активизация встроенного межсетевого экрана Windows и настройка его параметров		
	Практическое занятие 11. Настройка и использование межсетевого экрана в Windows	2	

	Самостоятельная работа 9. Составить сравнительную характеристику межсетевых экранов различных видов**.**	8	
Тема 3.3. Организация защиты виртуальных частных сетей (VPN)	**Содержание учебного материала**	6	ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 1.4, ПК 3.3, ДК 11.1, ДК 11.2
	1.Сущность технологии построения виртуальных частных сетей как современного средства построения защищённых каналов связи в ИС.Задачи, решаемые VPN.		
	2.Аппаратная и программная реализация виртуальных частных сетей.		
	3.Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне		
	4.Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP. Применение технологии терминального доступа. «VipNet.» Использование протокола IPSec для защиты сетей.		
	5.Установка и настройка VPN .средствами СЗИ		
	Практическое занятие 12. Создание VPN-подключения средствами Windows.	2	
Промежуточная аттестация в форме дифференцированного зачета		**2**	
Всего		**120**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

В целях реализации компетентностного подхода при изучении дисциплины ОП.11 Информационная безопасность персонального компьютера и компьютерных сетей используются активные и интерактивные формы проведения занятий (мультимедиа-презентации, деловые игры, разбор конкретных ситуаций, групповые дискуссии).

Применение на учебном занятии интерактивных форм работы, стимулирует познавательную мотивацию обучающихся, помогает поддержать мотивацию обучающихся к получению знаний, налаживанию позитивных межличностных отношений, помогает установлению доброжелательной атмосферы. Инициирование и поддержка исследовательской деятельности обучающихся в рамках реализации ими индивидуальных и групповых исследовательских проектов, дает возможность приобрести навык самостоятельного решения проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения.

Для позитивного восприятия обучающимися требований преподавателя, привлечения их внимания к обсуждаемой на занятии информации, активизации их познавательной деятельности на учебных занятиях между преподавателем и обучающимися устанавливаются доверительные отношения.

На учебном занятии соблюдаются общепринятые нормы поведения, правила общения со старшими (преподавателем) и сверстниками (обучающимися), принципы учебной дисциплины и самоорганизации.

3.1. Требования к минимуму материально-техническому обеспечению

Реализация программы учебной дисциплины обеспечена учебной лабораторией компьютерных сетей и телекоммуникаций для проведения лабораторных и практических занятий, междисциплинарной подготовки, оснащенным следующим оборудованием:

Перечень учебно - наглядных пособий:

Раздаточный материал: образцы разных типов кабельных сред

Оснащенность оборудованием:

- маршрутизатор D-Link[DIR-100].
- модем внутренний Zyxel OMNI 56K PCI Plus
- модем-маршрутизатор D-Link DSL-2610U ADSL+ беспроводной с 4 портами
- маршрутизатор Cisco 800
- маршрутизатор Zyxel
- коммутатор управляемый Dlink
- обжимной инструмент
- расходные материалы для монтажа СКС.
- коммутатор управляемый 2 уровня HP
- точка доступа WiFi доступа/маршрутизатор ASUS
- реконфигурируемое шасси на базе ПЛИС Xilinx Spartan-6 LX25 со встроенным контроллером реального времени 400 МГц и возможностью установки 4 модулей ввода/вывода сигналов
- устройство коммутации рабочих станций к сетям FastEthernet и GigabitEthernet4 шт.
- тренировочные рабочие места на базе ПК Pentium 4 – 10 комплектов.

ПК, мультимедийное оборудование:

- автоматизированные рабочие места на 10обучающихся (intelcorei3-3,3 GHz, 8 GbRAM, 2TbHDD, LED24”), с доступом к сети Интернет
- автоматизированное рабочее место преподавателя (i3-3,3 GHz, 8 Gb RAM, 2Tb HDD, LCD24”), с доступом к сети Интернет
- сервер HP DL380G5 E5310 Intel(R) Xeon(R) CPU 2x4x2.33GHz, 6144 mb, 149 Gb HDD.;

Учебная мебель: столы, стулья, доска меловая.

Программное обеспечение:

Microsoft Windows (договор № 7810 от 14.09.2021 до 30.11.2022), Microsoft Office Professional Plus (договор № 7810 от 14.09.2021 до 30.11.2022), Dip Trace Freeware, Cisco Packet Tracer (свободно распространяемое ПО), Microsoft Visual Studio Code (Свободно-распространяемое ПО), Oracle VM Virtual Box (свободно-распространяемое ПО)), Zoom (бесплатная версия) – свободно-распространяемое ПО.

3.2. Информационное обеспечение реализации программы

Для реализации программы учебной дисциплины библиотечный фонд имеет печатные и информационные ресурсы.

3.2.1. Основные источники:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/97562.html (дата обращения: 09.06.2022). — Режим доступа: для авторизир. пользователей.
2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837 (дата обращения: 09.06.2022).

3.2.2. Дополнительные источники:

1. Журнал «Вестник компьютерных и информационных технологий». [Текст : Электронный ресурс]: журнал / М. : Издательство ООО ИД Спектр 2019. - 60 с. - Режим доступа: https://elibrary.ru/contents.asp?id=39162311 (дата обращения: 09.06.2022).
2. Информационно-управляющие системы : научный журнал. - Санкт-Петербург : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2002 - . - Выходит раз в два месяца. - ISSN 1684-8853. - Текст : электронный. – URL: https://www.elibrary.ru/title_about.asp?id=25785 (дата обращения: 09.06.2022).

3.2.3. Информационные ресурсы:

1. http://www.iso27000.ru - Русскоязычный информационный портал, посвященный вопросам управления информационной безопасностью

2. http://www.studfiles.net/preview/2012615/- Информационная безопасность и ее составляющие
3. http://www.ot.ru/press20141106.html - Сайт, посвященный защите информации
4. http://www.geoline-tech.com/top-20-sites-about-information-security/ - Сайт, посвященный проблемам информационной безопасности

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (знания, умения, практический опыт)	**Критерии оценки**	**Методы оценки**
Знания:		
– понятие и составляющие информационной безопасности; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– формулировка основных определений информационной безопасности; – характеристика составляющих информационной безопасности	Самостоятельная работа № 1, Тест № 1 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– виды угроз информации и методы защиты от них; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– перечисление видов угроз информации; – выбор методов защиты от конкретной угрозы; – выбор средств защиты от конкретной угрозы	Самостоятельная работа № 3, Тест № 1 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– законы, стандарты и спецификации информационной безопасности; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– перечисление законов, стандартов и спецификаций информационной безопасности; – знание статей законов и порядка их применения; – знание стандартов и порядка их применения	Самостоятельная работа № 2, Тест № 2 Устный опрос, тестирование, накопительное оценивание (рейтинг))
– меры процедурного уровня информационной безопасности; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ДК 11.1, ДК 11.2	– перечисление мер процедурного уровня информационной безопасности; – характеристика каждой из мер процедурного уровня; – знание методов и средств защиты, используемых на процедурном уровне	Самостоятельная работа № 3, Тест № 2 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– меры программно-технического уровня информационной	– перечисление мер программно-технического уровня информационной безопасности	Тест № 2 Устный опрос, тестирование,

безопасности; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ДК 11.1, ДК 11.2		накопительное оценивание (рейтинг)
– методы защиты информации от несанкционированного доступа; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– применение методов защиты информации от несанкционированного доступа	Практическая работа № 1-4, Тест № 3 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– способы разграничения полномочий и доступа к объектам; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– использование способов разграничения полномочий и доступа к объектам	Практическая работа № 1-4, Тест № 3 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– осуществление регистрации и аудита в компьютерной системе; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– осуществление регистрации и аудита в компьютерной системе	Практическая работа № 4, Тест № 3 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– проведение оценки рисков компьютерной системы; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– проведение оценки рисков компьютерной системы	Самостоятельная работа № 2-3, Тест № 2 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– применение средств антивирусной защиты. ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– применение средств антивирусной защиты	Практическая работа № 7-8, Самостоятельная работа № 7-8, Тест № 4 Устный опрос, тестирование, накопительное оценивание (рейтинг)
Умения:		
– проводить анализ и оценку уязвимостей	– проведение анализа и оценки уязвимостей компьютерной системы;	Самостоятельная работа № 3, Тест № 1

компьютерной системы; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2		Устный опрос, тестирование, накопительное оценивание (рейтинг)
– применять меры информационной безопасности процедурного уровня; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– применение мер информационной безопасности процедурного уровня	Самостоятельная работа № 3, Тест № 1 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– осуществлять защиту информации от несанкционированного доступа; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– осуществление защиты информации от несанкционированного доступ	Практическая работа № 1-4, Тест № 3 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– настраивать безопасность почтового клиента; настраивать параметры аутентификации пользователей; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ДК 11.1	– настройка безопасности почтового клиента; настройка параметров аутентификации пользователей	Практическая работа № 1, Тест № 3 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– осуществлять регистрацию и аудит информационной безопасности; настраивать системы разграничения доступа; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– осуществление регистрации и аудита информационной безопасности; настройка системы разграничения доступа	Практическая работа № 1-4, Тест № 3. Устный опрос, тестирование, накопительное оценивание (рейтинг)
– применять криптографические методы и средства зашиты информации; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– применение криптографических методов и средств зашиты информации	Практическая работа № 5-6, Самостоятельная работа № 4-6, Тест № 4 Устный опрос, тестирование, накопительное

		оценивание (рейтинг)
– использовать средства антивирусной защиты; ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ПК 2.3, ПК 3.3, ДК 11.1, ДК 11.2	– использование средств антивирусной защиты	Практическая работа № 7-8, Самостоятельная работа № 7-8, Тест № 4 Устный опрос, тестирование, накопительное оценивание (рейтинг)
– использовать стандарты и спецификации информационной безопасности. ОК 1, ОК 2, ОК 3,ОК 4, ОК 5,ОК 9, ДК 11.1, ДК 11.2	– использование стандартов и спецификаций информационной безопасности	Самостоятельная работа № 2, Тест № 2 Устный опрос, тестирование, накопительное оценивание (рейтинг)
Практический опыт:		
– применения средств и методов защиты информации;	– демонстрирует навыки применения средств и методов защиты информации;	- Тестирование по всем темам; - Экспертная оценка самостоятельной работы; - Экспертная оценка практической работы; - Решение ситуационных задач.
– выбора, установки и настройки средств защиты информации;	– демонстрирует навыки выбора, установки и настройки средств защиты информации;	- Тестирование по всем темам; - Экспертная оценка самостоятельной работы; - Экспертная оценка практической работы; - Решение ситуационных задач.