Приложение к рабочей программе
по профессиональному модулю ПМ.03
Обеспечение информационной безопасности
многоканальных телекоммуникационных
систем и сетей электросвязи

Федеральное агентство связи
Уральский технический институт связи и информатики (филиал)
ФГБОУ ВО «Сибирский государственный университет
телекоммуникаций и информатики» в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УРАЛЬСКИЙ
ТЕХНИЧЕСКИЙ
ИНСТИТУТ
СВЯЗИ
И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
_____ Е.А. Субботин
«29» 06 2016 г.

Оценочные средства текущего контроля и промежуточной аттестации
по профессиональному модулю

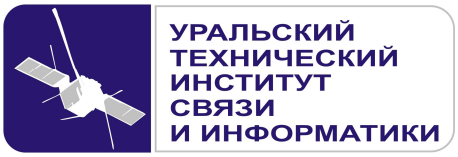
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

для специальности:
11.02.09 «Многоканальные телекоммуникационные системы»

Екатеринбург
2016

Приложение к рабочей программе
по профессиональному модулю ПМ.03
Обеспечение информационной безопасности
многоканальных телекоммуникационных
систем и сетей электросвязи

Федеральное агентство связи
Уральский технический институт связи и информатики (филиал)
ФГБОУ ВО «Сибирский государственный университет
телекоммуникаций и информатики» в г. Екатеринбурге
(УрТИСИ СибГУТИ)



УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
_____ Е.А. Субботин
«____» _____ 20__ г.

Оценочные средства текущего контроля и промежуточной аттестации
по профессиональному модулю

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

для специальности:
11.02.09 «Многоканальные телекоммуникационные системы»

Екатеринбург
2016

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол №10 от 29.06. 2016
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано:
Заместитель директора
по учебно-методической работе
_____ Е.А. Минина

Составитель: Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Рецензент: Татаркина О.А. - начальник станционного участка
Екатеринбургского филиала ПАО «Ростелеком»

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано:
Заместитель директора
по учебно-методической работе
_____ Е.А. Минина

Составитель: Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Рецензент: Татаркина О.А. - начальник станционного участка
Екатеринбургского филиала ПАО «Ростелеком»

Содержание

1 Общие положения 4
2 Формы контроля и оценивания элементов профессионального модуля 5
3 Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном) 6
4 Комплект материалов для оценки сформированности общих и профессиональных компетенций по виду профессиональной деятельности 8
Регистрация изменений в оценочных средствах текущего контроля и промежуточной аттестации по профессиональному модулю 21

1 Общие положения

Комплект оценочных средств предназначен для проверки результатов освоения профессионального модуля основной профессиональной образовательной программы по специальности 11.02.09 «Многоканальные телекоммуникационные системы» (базовой подготовки) среднего профессионального образования в части овладения видом профессиональной деятельности «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи».

Форма аттестации по профессиональному модулю - экзамен (квалификационный). Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Экзамен предусматривает выполнение практических заданий.

2 Формы контроля и оценивания элементов профессионального модуля

Таблица 1

Элемент модуля	Форма контроля и оценивания	
	Промежуточная аттестация	Текущий контроль
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи.	Дифференцированный зачет.	- проверка отчетов по практическим занятиям; - проверка выполнения самостоятельных работ; - проверка теоретических знаний по междисциплинарному курсу в форме тестирования.
МДК.03.02 Технология применения комплексной системы защиты информации.	Дифференцированный зачет.	- проверка отчетов по практическим занятиям; - проверка выполнения самостоятельных работ; - проверка теоретических знаний по междисциплинарному курсу в форме тестирования.
УП.03 Учебная практика.	Дифференцированный зачет.	Наблюдения во время выполнения заданий.
ПП.03 Производственная практика (по профилю специальности).	Дифференцированный зачет.	Наблюдения во время выполнения заданий.

Перечень зачетных тем по всем МДК

Таблица 2

Название МДК	Зачетные темы МДК	Форма контроля
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи.	Тема 1 Основы информационной безопасности.	Практические занятия, конспектирование учебного материала.
	Тема 2 Правовое обеспечение информационной безопасности.	Конспектирование учебного материала, Рефераты.
	Тема 3 Организационное обеспечение информационной безопасности.	Практические занятия, конспектирование учебного материала, отчеты по учебной практике.
МДК 03.02 Технология применения комплексной системы защиты информации.	Тема 1 Программно-аппаратные средства защиты информации.	Практические занятия, конспектирование учебного материала.
	Тема 2 Администрирование телекоммуникационных систем и сетей связи.	Практические занятия, конспектирование учебного материала, отчет по учебной и производственной практикам.

3 Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном)

В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций (Таблица 3):

Таблица 3

Код ПК, ОК	Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	Показатели оценки результата
ПК 3.1	Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.	- четкое понимание проблем информационной безопасности в сфере телекоммуникаций; - грамотное выявление, классификация и анализ угроз информационной безопасности и формы их проявления; - выбор механизмов и средств обеспечения информационной безопасности программных и программно-аппаратных; - грамотное оформление документации для лицензирования работ в области информационной безопасности; разработка политики в области информационной безопасности.
ПК 3.2	Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	- расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению; - владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; - владение технологией аутентификации; - обеспечение технологии защиты межсетевого обмена данными; построение системы антивирусной защиты систем телекоммуникационных систем.
ПК 3.3	Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.	- выбор и использование пакетов прикладных программ для безопасного администрирования сетевых операционных систем; обеспечение программными и программно-аппаратными методами безопасности сетей доступа, объединенных сетей и управления телекоммуникационными сетями.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	- своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения предшествующих тем, разделов, дисциплин, МДК, модулей.

ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в области обеспечения безопасности систем вещания; - оценка эффективности и качества выполнения самостоятельных и домашних заданий.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- решение стандартных и нестандартных профессиональных задач по обеспечению безопасности систем вещания.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	- эффективный поиск необходимой информации для решения задач в области сетевой безопасности; - использование учебной, справочной литературы, нормативно-правовых источников и Интернет-ресурсов.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- работа с различными операционными системами и средами, программно-аппаратными и программными средствами.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися и преподавателями в ходе обучения, а также с членами коллектива предприятия во время производственной практики; -внесение индивидуального вклада в коллективное решение задач.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	- самоанализ и коррекция результатов собственной работы, оценка деятельности по конечному результату.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- планирование и организация самостоятельного обучения при освоении профессионального модуля.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- анализ инноваций в области программного обеспечения, развития отрасли; - расширение кругозора в профессиональной деятельности.

4 Комплект материалов для оценки сформированности общих и профессиональных компетенций по виду профессиональной деятельности

В состав комплекта оценочных средств входят задания для экзаменующихся и критерии оценки выполненных заданий.

4.1 Задания для экзаменующихся

Количество вариантов - 10.

Оцениваемые компетенции: ПК 3.1 - ПК 3.3, ОК 1 - ОК 9.

Условия выполнения задания: учебная лаборатория.

Вариант 1

Задание 1

Выполнить расчеты для определения класса информационной системы передачи данных (ИСПДн).

Инструкция:

1) Выбрать населенный пункт (поселение) - Город Курган областной.
2) Используя ресурсы поисковой системы определить численность населения.
3) Определить объем данных, основываясь на численности населения.
4) Определить класс ИСПДн.
5) Выбрать средства защиты персональных данных (ПДн).

Перечень раздаточных и дополнительных материалов:

1) Классификация информационных систем персональных данных (ИСПДн).
2) http://weta.ru/kalkulyator_klassa_ispdn.php.
3) https://www.yandex.ru/

Задание 2

Настроить параметры локальной политики безопасности операционной системы Windows 7 (XP).

Инструкция:

1) Активизировать и настроить панель управления операционной системы Windows 7/XP.
2) Настроить политику паролей.
3) Настроить политику блокировки учетной записи.
4) Изменить пароль своей учетной записи.

Перечень раздаточных и дополнительных материалов:

1) Настройка параметров аутентификации Windows 7 (XP).

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 с. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 с. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 2

Задание 1

Разработать комплекс мероприятий на получение лицензии на определенный вид деятельности в области информационной безопасности.

Вид деятельности: Разработка и (или) производство средств защиты конфиденциальной информации (в пределах компетенции ФСБ).

Инструкция:

1) Использовать раздаточный материал.

2) Определить нормативные и правовые документы для лицензированного вида деятельности.

3) Определить степень секретности и виды конфиденциальной информации.

Перечень раздаточных и дополнительных материалов:

1) Виды деятельности, при которых необходима лицензия ФСБ.

2) Перечень документов для получения лицензии на деятельность по технической защите конфиденциальной информации.

3) Лицензирование деятельности по технической защите конфиденциальной информации.

4) https://www.yandex.ru/

5) http://www.consultant.ru/

Задание 2

1) Создать учетную запись пользователя.

2) Создать локальную группу пользователей.

3) Выполнить временную блокировку учетной записи.

Инструкция:

1) Создать учетную запись пользователя, локальную группу пользователей, используя раздаточный и дополнительный материал.

2) Изменить состав пользователей в локальной группе, используя раздаточный и дополнительный материал.

3) Выполнить временную блокировку учетной записи, используя раздаточный и дополнительный материал.

4) Записать в отчет последовательность команд (операций).

Перечень раздаточных и дополнительных материалов:

1) Назначение прав пользователей при произвольном управлении доступом.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 3

Задание 1

Разработать комплекс мероприятий на получение лицензии на определенный вид деятельности в области информационной безопасности.

Вид деятельности: Деятельность по технической защите конфиденциальной информации. Разработка и (или) производство средств защиты конфиденциальной информации.

Инструкция:

1) Использовать раздаточный материал.

2) Определить нормативные и правовые документы для лицензированного вида деятельности.

3) Определить степень секретности и виды конфиденциальной информации.

Перечень раздаточных и дополнительных материалов:

1) Виды деятельности, при которых необходима лицензия ФСБ.

2) Перечень документов для получения лицензии на деятельность по технической защите конфиденциальной информации.

3) Лицензирование деятельности по технической защите конфиденциальной информации.

4) https://www.yandex.ru/

Задание 2

Разработать систему видеонаблюдения, входящую в комплексную систему информационной безопасности.

Объект: Периметр одноэтажного здания.

Инструкция:

1) Составить описание и техническое задание на установку системы видеонаблюдения.

2) Составить план размещения видеокамер.

3) Выбрать видеооборудование по техническим характеристикам с учетом особенностей объекта контроля.

4) Составить схему подключения оборудования.

Перечень раздаточных и дополнительных материалов:

1) Принцип построения систем видеонаблюдения.

2) Проектирование системы видеонаблюдения.

3) Видеокамеры Arman.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 4

Задание 1

Разработать комплекс необходимых мероприятий по защите информации.

Объект: Помещение с компьютерным оборудованием (классом).

Инструкция:

1) Использовать перечень раздаточных и дополнительных материалов для составления технического задания на аттестацию объекта.

2) Выполнить последовательность действий для получения аттестата соответствия.

3) Составить отчетную документацию в виде протокола аттестационных испытаний (аттестата соответствия).

Перечень раздаточных и дополнительных материалов:

1) Положение об аттестации.
2) Техническое задание на аттестацию.
3) https://www.yandex.ru/

Задание 2

1) Выполнить установку антивирусного сервера и антивирусной консоли.
2) Выполнить установку антивирусного агента на компьютер.

Инструкция:

1) Установить антивирусный сервер и антивирусную консоль.
2) Установить антивирусный агент на компьютер.
3) Выполнить удаление отдельных компонентов комплекса.

Перечень раздаточных и дополнительных материалов:

1) Установка программного антивирусного комплекса Dr WEB.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 5

Задание 1

Составить техническое задание на аттестацию помещения. Разработать комплекс необходимой документации по защите информационной защите помещений.

Объект: Жилое помещение – квартиры, коттеджи.

Инструкция:

1) Пояснить методику составления технического задания на аттестацию помещения, используя раздаточный и дополнительный материал.

2) Выполнить последовательность действий для получения аттестата соответствия.

3) Составить отчетную документацию в виде протокола аттестационных испытаний (аттестата соответствия).

Перечень раздаточных и дополнительных материалов:

1) Аттестация защищаемых помещений.
2) Положение об аттестации P_1994.11.25.
3) Требования к помещениям.
4) https://www.yandex.ru/

Задание 2

1) Установить на компьютер антивирусную программу KFA16.0.1.445 ru в стандартном режиме.
2) Установить на компьютер антивирусную программу KFA16.0.1.445ru из командной строки.
3) Выполнить выборочную проверку файлов/папок антивирусной программой KFA.

Инструкция:

1) Изучить функциональные возможности антивирусной программы KFA, используя раздаточный и дополнительный материал.
2) Выполнить пошаговую установку антивирусной программы.
3) Выполнить установку антивирусной программы из командной строки.

Перечень раздаточных и дополнительных материалов:

1) Описание антивирусной программы Kaspersky Free Anti-Virus.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 6

Задание 1

Провести аудит информационной системы предприятия.

Объект: Отдел материально-технического обеспечения организации.

Инструкция:

1) Пояснить методику проведения анализа информационных ресурсов в организации, используя раздаточный и дополнительный материал.

2) Определить основные угрозы безопасности и их источники.

3) Сформировать неформальную модель возможных нарушителей и составить план мероприятий по нейтрализации угроз.

Перечень раздаточных и дополнительных материалов:

1) Модель системы информационной безопасности (ИБ) на предприятии.

2) Мероприятия по защите автоматизированных систем (АС).

3) https://www.yandex.ru/

Задание 2

1) Настроить межсетевой экран операционной системы Windows 7 (XP).

2) Установить межсетевой экран (Firewall) Comodo Firewall на компьютер.

Инструкция:

1) Активизировать и настроить встроенный брандмауэр операционной системы Windows XP, используя раздаточный и дополнительный материал.

2) Установить и настроить межсетевой экран Comodo Firewall, используя раздаточный и дополнительный материал.

Перечень раздаточных и дополнительных материалов:

1) Активизизация встроенного брандмауэра операционной системы Windows XP и настройка его параметров.

2) Установка и настройка межсетевого экрана Comodo Firewall.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 7

Задание 1

Провести аудит программно-технических средств организации. Выполнить анализ и определить основные угрозы. Разработать модель системы информационной безопасности.

Объект: Отдел материально-технического обеспечения организации.

Инструкция:

1) Определить основные угрозы безопасности и их источники.

2) Составить неформальную модель возможных нарушителей.

3) Разработать план мероприятий по формированию режима безопасности информации в организации.

Перечень раздаточных и дополнительных материалов:

1) Программные и технические средства.

2) Программные и технические методы защиты.

3) https://www.yandex.ru/

Задание 2

1) Выполнить шифрование исходного текста из таблицы 1 методом перестановки.

2) Выполнить шифрование исходного текста из таблицы 3 методом гаммирования.

Инструкция:

1) Записать исходные данные для шифрования, используя раздаточный и дополнительный материал.

2) Изучить задания к выполнению работы.

3) Выполнить задания, используя раздаточный и дополнительный материал.

Перечень раздаточных и дополнительных материалов:

1) Таблица 1 – Исходные данные в виде открытого текста.

2) Таблица 2 – Открытый ключ.

3) Таблица 3 – Открытый текст для преобразования гаммированием.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный

центр – ВНИИЭФ, 2015. - 224 с. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 8

Задание 1

Провести аудит программно-технических средств предприятия. Выполнить анализ и разработать модель угроз. Разработать политику системы информационной безопасности.

Объект: Больницы, поликлиники, амбулатории, диспансеры.

Инструкция:

1) Изучить порядок проведения анализа программно-технических ресурсов предприятия, используя раздаточный и дополнительный материал.

2) Определить состав программно-технического оборудования и возможные основные угрозы безопасности.

3) Сформулировать рекомендации и план мероприятий по нейтрализации угроз.

4) Описание политики безопасности предприятия.

Перечень раздаточных и дополнительных материалов:

1) Безопасность предприятия.

2) Петренко_Политики информационной безопасности.

3) https://www.yandex.ru/

Задание 2

1) Выполнить шифрование/расшифрование системой EFS.

2) Сгенерировать ключи шифрования (открытый и закрытый) и поместить их в сертификат для экспорта.

Инструкция:

1) Изучить основные сведения о шифрующей системе EFS, , используя раздаточный и дополнительный материал.

2) Выбрать файл (папку с файлами) для шифрования.

3) Выполнить шифрование выбранных файлов, используя команды и диалоговые окна.

4) Выполнить расшифрование, используя диалоговые окна и соответствующие команды.

5) Получить сертификат для экспорта ключей для расшифрования данных на другом компьютере.

Перечень раздаточных и дополнительных материалов:

1) Основные сведения о EFS.

2) Шифрование файлов.

3) Сертификаты.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 9

Задание 1

Определить текущее состояние помещения с точки зрения технической защищенности объекта информатизации. Составить поэтапный план мероприятий по защите информации: 1) подготовительный, предпроектный; 2) проектирование системы технической защиты информации; 3) этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации.

Объект: Архив организации.

Инструкция:

1) Изучить порядок проведения анализа, используя раздаточный и дополнительный материал.

2) Провести обследование защищаемых объектов, определить категорию помещения, как объекта защиты.

3) Разработать аналитическое обоснование необходимости создания системы технической защиты информации и техническое задание на ее создание.

Перечень раздаточных и дополнительных материалов:

1) Анализ защищаемых помещений и каналов утечки.

2) защищаемые помещения.

3) ЗИ от утечек по техническим каналам.

Задание 2

1) Провести анализ функциональных возможностей программных продуктов для защиты информационной системы.

2) Установить и проанализировать работу программы ViPNet Registration Point.

3) Изучить возможности программы Sentinel HASP.

4) Протестировать ключи Guardant SP.

Инструкция:

1) Изучить состав линейки программных продуктов компании «Инфо-ТеКС», используя раздаточный и дополнительный материал.

2) Изучить назначение, технические возможности электронных ключей защиты, используя раздаточный и дополнительный материал.

3) Установить программы Sentinel HASP и Guardant SP, изучить интерфейс и защитные функции.

Перечень раздаточных и дополнительных материалов:

1) Продуктовая линейка CUSTOM.

2) Электронные ключи защиты.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

Вариант 10

Задание 1

Разработать систему видеонаблюдения, входящую в комплексную систему информационной безопасности.

Объект: Периметр одноэтажного здания.

Инструкция:

1) Составить описание и техническое задание на установку системы видеонаблюдения.

2) Составить план размещения видеокамер.

3) Выбрать видеооборудование по техническим характеристикам с учетом особенностей объекта контроля.

4) Составить схему подключения оборудования.

Перечень раздаточных и дополнительных материалов:

1) Принцип построения систем видеонаблюдения.

2) Проектирование системы видеонаблюдения.

Задание 2

1) Изучить принципы действия, конструкцию и характеристики датчиков.

2) Изучить принцип контроля линейно-кабельных сооружений оператора связи МАКС ЛКС.

3) Изучить применение датчиков на сайте ТехноТроникс.

4) Составить схему размещения различных датчиков контроля состояния линейного оборудования на местной сети связи.

Инструкция:

1) Рассмотреть принцип работы системы контроля линейно-кабельных сооружений, используя раздаточный и дополнительный материал.

2) Рассмотреть применение датчиков ТехноТроникс в системе контроля линейно-кабельных сооружений.

Перечень раздаточных и дополнительных материалов:

1) Датчик вскрытия и запыленности.

2) Контроль линейно-кабельных сооружений.

3) Руководство пользователя Мираж_GE_RX4_01.

Возможно использование литературы:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Максимальное время выполнения заданий: 35 минут (20 минут на подготовку и 15 минут на ответ).

4.2 Критерии оценки выполненных заданий

Выполнение задания:

- самостоятельность выполнения задания;

- рациональное распределение времени на выполнение задания (обязательно наличие следующих этапов выполнения задания: ознакомление с заданием и планирование работы; получение информации; подготовка продукта; рефлексия выполнения задания и коррекция подготовленного продукта перед сдачей);

- обращение в ходе выполнения задания к информационным источникам;
- своевременность выполнения заданий в соответствии с установленным лимитом времени;
- грамотность представления выполненного задания.

Подготовленный продукт:

Код ПК, ОК	Наименование компетенции	Выполнил	Не выполнил
ПК 3.1	Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.		
ПК 3.2	Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.		
ПК 3.3	Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.		
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.		

Регистрация изменений в оценочных средствах текущего контроля и промежуточной аттестации по профессиональному модулю

№ п/п	Учебный год	Содержание изменений	Преподаватель	Решение цикловой комиссии (№ протокола, дата, подпись ПЦК)