АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Корпоративной защиты от внутренних угроз информационной безопасности

название учебной дисциплины

1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**, входящей в укрупненную группу специальностей **10.00.00 Информационная безопасность**.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании и в программах профессиональной подготовки обучающихся укрупненной группы специальностей **10.00.00 Информационная безопасность**.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Корпоративная защита от внутренних угроз информационной безопасности» принадлежит к математическому и общему естественнонаучному циклу и связана с учебными дисциплинами:

- МДК. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты;
- МДК. Криптографическая защита информации.
- Эксплуатация информационно-телекоммуникационных систем и сетей;
- Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.

3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате изучения предмета студент должен освоить основной вид профессиональной деятельности «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» и соответствующие ему профессиональные компетенции и общие компетенции.

4. Рекомендуемое количество часов на освоение программы дисциплины

Максимальная учебная нагрузка обучающегося 88 часов.

- 40 часов вариативной части, направленных на усиление обязательной части программы.

5. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	**Объем часов**
Максимальная учебная нагрузка (всего)	**88**
Обязательная аудиторная учебная нагрузка (всего)	**40**
в том числе:	
- лабораторные работы	не предусмотрено
- практические занятия	40
- курсовая работа (проект)	не предусмотрено
Самостоятельная работа обучающегося	**8**
в том числе:	

- самостоятельная работа над курсовой работой (проектом)	не предусмотрено
- изучение тем.	2
Итоговая аттестация в форме экзамена	

6. Содержание дисциплины

Тема 1 Linux. QNX и другие операционные системы.

Тема 2-3. Bash, структуры, пути.

Тема 4. Использование команд Linux

Тема 5. Управление аккаунтами в Linux

Тема 6. Создание ссылок и удаление файлов.

Тема 7. Использование джокеров

Тема 8. Регулярные выражения

Тема 9. FHS и поиск файлов

Тема 10. Стандарт иерархии файловой системы

Тема 11. Модули ядра

Тема 12. Системная и сетевая документация

Тема 13. Типы системной документации в Linux

Тема 14. Модель прав доступа в Linux

Тема 15. Протокол TCP/IP

Тема 16. Служба DNS

Тема 17. Служба каталогов Active Directory. Служба файлов и печати

Тема 18. Сетевые протоколы и службы. Служба резервного копирования

Тема 19. Службы терминалов. Мониторинг

Тема 20. Модель OSI

Тема 21. Физический, канальный и сетевой уровень

Тема 22. Транспортный, сеансовый, предоставления и прикладной уровень

Тема 23. Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем.

Тема 24. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.

Тема 25. Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy.

Тема 26. Конфигурирование DLP IWTM
Исправление типовых неисправностей.

Тема 27. Технологии агентского мониторинга

Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом

Тема 28. Политики агентского мониторинга, особенности их настройки. Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий;

Тема 29. Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата.

Тема 30. Разработка политик безопасности, анализ выявленных инцидентов

Тема 31. Разработка и тестирование политик в системе DLP IWTM. Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с

категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами;

Тема 32. Мониторинг трафика. Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером.