Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ЛЕСОСИБИРСКИЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ –
филиал Сибирского федерального университета

Утверждаю
Заведующий кафедрой высшей
математики, информатики
и естествознания
_____Л.Н. Храмова
«22» 09 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина «Защита информации в компьютерных сетях»
Дополнительная образовательная программа профессиональной переподготовки «Информационная безопасность и компьютерная безопасность»

Лесосибирск, 2020

1. Цель освоения дисциплины – формирование у обучающихся знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи:

– формирование представления о методах и средствах защиты информации в компьютерных сетях;

– формирование представления о технологии межсетевого экранирования;

– формирование умения построения виртуальных частных сетей.

2. Планируемые результаты обучения

В результате освоения дисциплины обучающийся должен знать:

– технологии обнаружения компьютерных атак и их возможности;

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

– особенности реализации методов защиты информации современными программно-аппаратными средствами.

В результате освоения дисциплины обучающийся должен уметь:

– выполнять функции администратора безопасности защищенных компьютерных систем;

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

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

В результате освоения дисциплины обучающийся должен владеть:

– средствами администрирования сетевых программно-аппаратных комплексов защиты информации;

– средствами администрирования систем обнаружения компьютерных атак;

– средствами администрирования систем организации виртуальных частных сетей.

3. Содержание дисциплины

3.1 Содержание дисциплины по программе, общая трудоемкость которой составляет 510 часов.

№ п/п	Наименование темы и ее содержание	Количество часов

№ п/п	Наименование темы и ее содержание	Количество часов
1	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. 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.	20
2	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. 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. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации.	25
3	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. 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.	25
Итого		70

3.2 Содержание дисциплины по программе, общая трудоемкость которой составляет 260 часов.

№ п/п	Наименование темы и ее содержание	Количество часов
1	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА.	15

№ п/п	Наименование темы и ее содержание	Количество часов
	Стандартизация в области обнаружения атак. 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.	
2	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. 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. Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации.	15
3	Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server 2003. Настройка сервера MSTS. Настройка протокола RDP. 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.	20
Итого		50

4. Оценочные средства

Форма аттестации – экзамен.

Вопросы к экзамену:

1.Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак.

2.Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы.

3.Атаки с использованием промежуточных узлов и территорий.

4.Технологии обнаружения компьютерных атак и их возможности.

5.Прямые и косвенные признаки атак.

6.Методы обнаружения атак.

7.Сигнатурный анализ и обнаружение аномалий.

8.Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА.

9.Стандартизация в области обнаружения атак. Архитектура СОА.

10.Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования.

11.Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА

12.Стратегии и средства межсетевого экранирования.

13.Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.

14.Требования руководящих документов ФСТЭК России к межсетевым экранам.

15.Обзор документов RFC, регламентирующих использование межсетевых экранов.

16.Типы межсетевых экранов. Схемы межсетевого экранирования.

17.Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров.

18.Понятие демилитаризованной зоны.

19. Укрепленный компьютер бастионного типа.

20. Организация узлов для отвлечения внимания злоумышленника.

21.Особенности фильтрации различных типов трафика.

22.Пакетный фильтр на базе ОС Windows 2000-XP.

23.Служба RRAS. Программа управления службой RRAS.

24.Шлюзы прикладного уровня. Сервер SQUID, принципы работы, варианты конфигурации.

25.Применение технологии терминального доступа. Общие сведения о технологии терминального доступа.

26.Обеспечение безопасности сервера ОС Windows Server 2003.

27.Настройка сервера MSTS.

28.Настройка протокола RDP. Службы каталогов. Общие сведения о службах каталогов.

29.Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Синадский, Н.И. Защита информации в компьютерных сетях: учебное пособие / Н.И. Синадский. – Екатеринбург, 2015.

2.Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учебник / П.Б. Хорев. – Москва, 2016.

Дополнительная литература:

3.Синадский, Н.И. О.Н. Угрозы безопасности компьютерной информации / Н.И. Синадский, О.Н. Соболев. – Екатеринбург, 2016.

Разработчик:
Заведующий кафедрой ВМИиЕ,
профессор, кандидат экономических наук,
доцент Л.Н. Храмова

Кандидат педагогических наук,
старший преподаватель кафедры ВМИиЕ А.В. Фирер
Согласовано:

Согласовано:
Декан ФДО Л.С. Шмульская