АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Технологии защиты информации в глобальных сетях»

по основной профессиональной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата)

Направленность (профиль): Организация и технология защиты информации
Общий объем дисциплины – 6 з.е. (216 часов)
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

- ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
- ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации;
- ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты;

Содержание дисциплины:
Дисциплина «Технологии защиты информации в глобальных сетях» включает в себя следующие разделы:
Форма обучения очная. Семестр 6.
Объем дисциплины в семестре – 3 з.е. (108 часов)
Форма промежуточной аттестации – Экзамен
1. Введение в глобальные вычислительные сети.. Тема 1. Операционные возможности глобальных вычислительных сетей. Мультисервисная (конвергентная) сеть. Основные задачи администратора при проектировании, построении и сопровождении сети. Назначение основных сервисов глобальных вычислительных сетей, их особенности реализации и использования.
Тема 2. Служба доменных имен. Терминология и принципы работы. Типы серверов доменных имен (Master, Slave, Cache, Stealth, Root). Понятие зон – прямая и обратная. Конфигурирование DNS в различных сетевых операционных системах. Протокол DNS..
2. Маршрутизация.. Тема 1. Организация взаимодействия в глобальных вычислительных сетях. Маршрутизация. Пересылка пакетов. Маршрутизатор и принципы его работы. Интерфейсы маршрутизатора. Введение в таблицу маршрутизации. Directly-Connected сети. Next-hop и выходной интерфейс. Статическая маршрутизация. Протоколы ARP и RARP. Суммирование статических маршрутов. Маршрут по умолчанию. Тема 2. Динамическая маршрутизация. Протоколы динамической маршрутизации. Классификация протоколов динамической маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протоколы маршрутизации состояния связей. Классовая и без классовая маршрутизация. Тема 3. Понятие сходимости протокола маршрутизации. Принципы работы таблицы маршрутизации. Лучший маршрут и метрика. Распределение нагрузки. Административная дистанция. Дистанционно-векторные протоколы динамической маршрутизации RIP, EIGRP. Протоколы маршрутизации состояния связей OSPF..
3. Почтовая служба. Тема 1. Организация почтовой службы. Основные способы организации (on-line, off-line). Средства реализации почтовой службы в различных сетевых операционных системах (sendmail, exim, postfix, Microsoft Exchange Server). Протоколы обмена почтовыми сообщениями (POP, SMTP, IMAP). Тема 2. Организация служб электронного общения в режиме on-line. Мессенджеры и VoIP сервис. Телеконференции. Группы новостей..
4. Программное обеспечение прикладного уровня.. Тема 1. Приложения, сервисы. Модель «клиент-сервер». Point-to-Point сети и приложения. Протоколы прикладного уровня: Web - HTTP (80) и HTTPS (443), Протоколы файлового обмена – FTP (20, 21) и SMB (445), электронной почты – SMTP (25), POP (110) и IMAP (143), дистанционного управления – Telnet (23), RDP (3389) и SSH (22), система доменных имён – DNS (53), протокол динамической конфигурации узла DHCP (67, 68), протоколы управления – SNMP (161, 162). Формат данных HTTP, FTP, SMTP, POPv3, DNS, DHCP и принцип их работы. Тема 2. Уровень защищённых сокетов, протокол SSL и его

применение. Принцип работы протокола SSL. Аутентификация и обмен ключами. Почтовая система (MUA, MTA, MDA). Виды конференцсвязи (аудио, видео), примеры организации конференций..

Форма обучения очная. Семестр 7.

Объем дисциплины в семестре – 3 з.е. (108 часов)

Форма промежуточной аттестации – Экзамен

5. Обеспечение безопасности межсетевого взаимодействия.. Тема 1. Межсетевое взаимодействие. Основы сетевого и межсетевого взаимодействия. Классификация сетевых атак. Информационная безопасность.

Тема 2. Политика безопасности. Шаблоны политики безопасности. Сетевая политика безопасности. Эшелонированная оборона

Тема 3. Управление рисками. Основные понятия. Процесс оценки рисков. Уменьшение рисков. Аудит информационной безопасности. Механизмы и службы защиты.

Тема 4. Определение информационных ресурсов, подлежащих защите, угроз безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

6. Межсетевые экраны.. Тема 1. Классификация межсетевых экранов. Пакетные фильтры. Пример набора правил пакетного фильтра. Пакетный фильтр с учетом контекста (Stateful Packet Inspection). Межсетевые экраны host-based. Прокси-сервер прикладного уровня.

Тема 2. Различные типы окружений межсетевых экранов. Основные принципы построения окружения межсетевого экрана. Конфигурация с одной DMZ-сетью. Конфигурация Service Leg. Конфигурация с двумя DMZ-сетями..

7. Виртуальные частные сети.. Тема 1. Виртуализация. Гипервизоры (Microsoft Hyper-V, VMware ESX, VirtualBOX). Технологии распределённых вычислений. Облачные вычисления. Кластеры. Диагностика сетей (программные, аппаратные и программно-аппаратные комплексы для тестирования и сопровождения сетей).

Тема 2. Виртуальные частные сети (VPN). Туннелирование. Протоколы VPN канального уровня. Протокол PPTP. Протокол L2TP. Протокол IPSec. Ассоциация обеспечения безопасности.

Тема 3. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH. Основные типы защищенных связей. Протоколы VPN транспортного уровня. Протокол SSL. Протокол SOCKS..

8. Системы обнаружения вторжений (Intrusion Detection Systems).. Тема 1. Типы IDS. Архитектура IDS. Способы управления. Информационные источники. Анализ, выполняемый IDS. Возможные ответные действия IDS. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. Цели и задачи использования IDS. Существующая политика безопасности. Развертывание IDS. Сильные стороны и ограниченность IDS. Тема 2. Участие в проведении экспериментальных исследований системы защиты информации..

Разработал:
доцент
кафедры ИВТиИБ Е.В. Шарлаев
Проверил:
Декан ФИТ А.С. Авдеев