АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Информационная безопасность компьютерных систем и сетей»

по основной профессиональной образовательной программе по направлению подготовки 09.03.04 «Программная инженерия» (уровень бакалавриата)

Направленность (профиль): Разработка программно-информационных систем
Общий объем дисциплины – 2 з.е. (72 часов)
Форма промежуточной аттестации – Зачет.
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

- ОПК-1: владением основными концепциями, принципами, теориями и фактами, связанными с информатикой;
- ПК-2: владением навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных;

Содержание дисциплины:
Дисциплина «Информационная безопасность компьютерных систем и сетей» включает в себя следующие разделы:
Форма обучения очная. Семестр 8.
1. Обеспечение безопасности в компьютерных системах и сетях. методы использования операционных систем, сетевых технологий, в том числе, основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах. Основные концепции, принципы, и факты информатики, связанные с безопасностью ОС. Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.
Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Сетевые угрозы, уязвимости и атаки. Средства защиты сетей..
2. Назначение, возможности, и основные защитные механизмы межсетевых экранов (МЭ). Методы использования сетевых технологий, в том числе, назначение и виды МЭ. Основные защитные механизмы, реализуемые МЭ. Основные возможности и варианты размещения МЭ. Достоинства и недостатки МЭ. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, script rejection, проверка почты, виртуальные частные сети, противодействие атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции. Общие рекомендации по применению. Политика безопасности при доступе к сети общего пользования. Демилитаризованная зона. Назначение, особенности и типовая схема "HoneyNet"..
3. Анализ содержимого почтового и Web-трафика (Content Security). Методы использования сетевых технологий, в том числе, использование систем анализа содержимого. Компоненты и функционирование систем контроля контента (электронная почта и HTTP-трафик). Политики безопасности, сценарии и варианты применения и реагирования..
4. Виртуальные частные сети (VPN). Методы использования сетевых технологий, в том числе, назначение, основные возможности, принципы функционирования и варианты реализации VPN. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению. Решение на базе ОС Windows. VPN на основе аппаратно-программных комплексов шифрования. Угрозы, связанные с использованием VPN..
5. Антивирусные средства защиты. Методы использования операционных систем, в том числе, общие правила применение антивирусных средств. Технологии обнаружения вирусов. Возможные варианты размещение антивирусных средств. Антивирусная защита, как средство нейтрализации угроз..
6. Обнаружение и устранение уязвимостей. Основные концепции, принципы работы и классификация средств анализа защищенности. Место и роль в общей системе обеспечения безопасности. Сравнение возможностей с межсетевыми экранами. Средства обеспечения адаптивной сетевой безопасности. Варианты решений по обеспечению безопасности сети организации. Обзор средств анализа защищенности сетевого уровня и уровня узла.

Специализированный анализ защищенности..

7. Мониторинг событий безопасности. Методы использования журналов событий в операционных системах и сетевых технологиях. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий. Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак..

8. Безопасность IP-телефонии. Методы использования сетевых технологий для передачи голоса и их защита. Основные понятия и определения VoIP. Основные протоколы VoIP. Уязвимости и атаки на VoIP. Инвентаризация VoIP сети. Перехват VoIP-трафика. Манипулирование в системах VoIP. Атаки на протокол передачи трафика реального времени RTP (Real-Time Protocol). Спам в VoIP-сетях. Механизмы обеспечения безопасности IP-телефонии. Планирование защищённой сетевой инфраструктуры IP-телефонии. Анализ защищенности VoIP. Криптографическая защита в VoIP сетях..

9. Безопасность беспроводных сетей. Методы использования беспроводных технологий и их защита. Общие сведения. Введение. Базовые механизмы защиты данных в беспроводных сетях. Защита беспроводных сетей на сетевом уровне. Стандарты WPA (Wi-Fi Protected Access) и 802.11i. Обнаружение атак в беспроводных сетях. Анализ защищённости беспроводных сетей. Сети WPAN. Безопасность Bluetooth. Организация гостевого доступа. Беспроводной доступ с использованием мобильных устройств..

Разработал:
доцент
кафедры ПМ В.С. Троицкий
Проверил:
Декан ФИТ А.С. Авдеев