АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Безопасность и защита информации в информационных системах»

по основной профессиональной образовательной программе по направлению подготовки 09.04.01 «Информатика и вычислительная техника» (уровень магистратуры)

Направленность (профиль): Программно-техническое обеспечение автоматизированных систем
Общий объем дисциплины – 4 з.е. (144 часов)
Форма промежуточной аттестации – Экзамен.
В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:

- ОПК-5.1: Выбирает средства автоматизации разработки и модернизации программного и аппаратного обеспечения;
- ОПК-6.1: Разрабатывает компоненты программно-аппаратных комплексов обработки информации;

Содержание дисциплины:
Дисциплина «Безопасность и защита информации в информационных системах» включает в себя следующие разделы:
Форма обучения очная. Семестр 2.
1. Обеспечение безопасности межсетевого взаимодействия. Разработка и модернизация программного и аппаратного обеспечения информационных и автоматизированных систем в области обеспечения их безопасности.. 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. Определение информационных ресурсов, подлежащих защите. Средства автоматизации разработки и модернизации программного и аппаратного обеспечения.
2. 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..
3. 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..
4. Системы обнаружения вторжений (Intrusion Detection Systems).. 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..

Разработал:
доцент
кафедры ИВТиИБ Е.В. Шарлаев

Проверил:
Декан ФИТ А.С. Авдеев