АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Организация и технология защиты информации»

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

Направленность (профиль): Разработка программно-информационных систем
Общий объем дисциплины – 3 з.е. (108 часов)
Форма промежуточной аттестации – Зачет.
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

- ПК-1: готовностью применять основные методы и инструменты разработки программного обеспечения;
- ПК-4: владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества;

Содержание дисциплины:
Дисциплина «Организация и технология защиты информации» включает в себя следующие разделы:
Форма обучения очная. Семестр 6.
1. Введение и организационно-правовые механизмы обеспечения информационной безопасности. Основные понятия и определения. Информация в компьютерных сетях и ее свойства. Виды и источники угроз информационной безопасности. Основные направления обеспечения информационной безопасности. Комплексный подход к обеспечению информационной безопасности. Меры противодействия угрозам безопасности (Морально-этические меры, правовые меры, организационные меры, технологические меры, технические меры, физические меры и.др.). Концепция информационной безопасности. Формальная теории защиты информации. Концепции и атрибуты качества программного обеспечения, в том числе, критерии оценки защищенности систем.
Информация как товар. Экономические проблемы информационной защиты. Страхование как метод защиты информации. Экономическая эффективность защиты информации. Виды ущерба от несанкционированного доступа (НСД) к информации. Методы оценки ущерба от НСД. Основные методы определения затрат на информационную безопасность. Оценка экономического эффекта защиты информации. Экономическая эффективность инвестиций в защиту информации.
Правовое обеспечение информационной безопасности. Информация как объект правового регулирования. Законодательство РФ в области информационной безопасности. Лицензирование и сертификация в области информационной безопасности. Компьютерные правонарушения. Основы организационного обеспечения информационной безопасности..
2. Криптографические методы защиты информации. Использование криптографических методов и соответствующих инструментальных средств защиты информации в существующих и разрабатываемых приложениях. Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Стеганографические методы защиты конфиденциальности. Стойкость криптографических систем и алгоритмов (теоретическая, практическая, вычислительная). Элементы криптоанализа.
Современные симметричные и асимметричные криптосистемы. Симметричные криптосистемы. Основные свойства симметричных криптосистем. Блочные и поточные шифры. Шифры DES, AES, ГОСТ 28147-89, режимы работы блочных шифров. Поточные шифры.
Асимметричные криптосистемы. Основные свойства асимметричных криптосистем. Однонаправленные функции. Общая схема функционирования систем с открытыми ключами. Криптосистема RSA и криптография с использованием эллиптических кривых. Комбинированные криптосистемы. Надежность криптосистем.
Функции хэширования. Основные свойства хэш-функций. Функция хэширования SHA, MD5, ГОСТ Р 34.11-94. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Ключевые и бесключевые функции хэширования.

Управление ключами. Генерация и хранение ключей. Распределение ключей. Выбор ключа, время жизни ключа, разделение секрета. Схемы обмена секретными ключами. Управление ключами в системах с открытым ключом.
Методы обеспечения целостности. Электронно-цифровая подпись(ЭЦП). Схема ЭЦП. Электронные сертификаты. Назначение. Схемы управления: централизованная (стандарт X509), распределённая (стандарт OpenPGP). Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи. Примеры применения ЭЦП и электронных сертификатов (IPSec, VPN, Электронные деньги и пр.)..
3. Безопасность компьютерных систем и сетей. Использование инструментальных средств защиты информации в сетевых приложениях. Общие вопросы безопасности в ЛВС. Классификация сетевых атак. Средства защиты. Аутентификация и управление идентификациями. Аутентификация на основе одноразовых и многоразовых паролей. Биометрическая идентификация и аутентификация пользователя. Аутентификация, основанная на симметричных и асимметричных алгоритмах. Протоколы аутентификации и идентификации. Взаимная проверка подлинности. Протоколы обмена и распределения ключей. Хранение учетных записей.
Основные схемы сетевой защиты. Сегментирование сетей на канальном уровне. Межсетевые экраны. Системы обнаружения и предотвращения проникновений. Приоритезация трафика и создание альтернативных маршрутов. Технологии туннелирования.
Принципы и средства защиты электронной почты, Web-технологий, VoIP, Wifi.
Вредоносное программное обеспечение. Классификация вредоносного ПО, механизмы его воздействия на телекоммуникационные и вычислительные системы. Методы и средства борьбы с вредоносным ПО.
Резервное копирование. Подсистема хранения данных. Уровни резервного копирования. Виды резервного копирования. Резервное копирование на физическом уровне, технология RAID. Надёжное удаление информации с носителей. Методы и инструменты разработки программного обеспечения для защиты информации. Концепции и атрибуты качества создаваемого программного обеспечения.

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