Информационная безопасность

Программа дисциплины, структурированная по темам

Введение.

Понятие информационной безопасности. Актуальность защиты информации, хранящейся и обрабатываемой в информационных системах различного назначения. Законодательная база деятельности в рассматриваемой области. Закон о государственной тайне и правила работы с секретными документами. КОАП, УК. Персональные данные и актуальность их защиты; обезличивание персональных данных, ограниченность этого подхода к защите ПД. Закон об ЭЦП и юридическая значимость ИС различного назначения (электронная торговля, электронный документооборот).

Виды атак на информационные системы.

Сетевые вторжения. Атаки с использованием Интернет. Вредоносные программы – вирусы, троянцы. Атаки типа «отказ в обслуживании». Несанкционированный доступ к данным.

Способы защиты информации.

Основные понятия криптографии: симметричные и несимметричные алгоритмы шифрования, вычисление хэш-значений, электронно-цифровая подпись (ЭЦП). Использование готовых криптосредств: Криптопро, Верба, CryptoAPI и криптопровайдеры. Классификация способов защиты информации: организационные, инженерно-технические (межсетевые экраны, замки, шифраторы), программные. Средства безопасности, встроенные в Windows. Модели разграничения доступа: дискреционная, ролевая и мандатная. Системы обнаружения вторжений. СЗИ прикладных ИС: идентификация и аутентификация; реакция на события в системе (протоколирование, оповещения, блокировки); разграничение доступа; контроль целостности данных и ПО;

Требования к средствам защиты.

Понятие о политике безопасности как основе для формулирования требований к системе защиты (модели угроз и нарушителя, субъекты и объекты защиты, принципы разграничения доступа). Общая классификация требований (конфиденциальность, целостность и доступность). Классификация информационных систем и средств вычислительной техники ФСТЭК РФ. Зависимость требований от класса системы.

Проектирование информационных систем в защищенном исполнении.

Этапы работы над системой: обследование, подготовка Техзадания, эскизное проектирование, техническое проектирование, разработка, документирование,

тестирование, опытная эксплуатация, промышленная эксплуатация. Формулирование политики безопасности. Задание по безопасности и профиль безопасности. Взаимодействие средств защиты информационной системы, базы данных и операционной системы. Понятие доверенной системы. Особенности архитектуры и программно-технической реализации: выделение Диспетчера доступа, использование идентификации Windows, применяемые сетевые протоколы.

Сертификация программных продуктов.

Общие сведения о системе сертификации информационных систем и средств вычислительной техники в РФ: цель сертификации, нормативные документы, выполняемые проверки.