КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

ТЕМА 6: ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Информационная безопасность – состояние защищенности информационной среды (инфосферы) общества, обеспечение её формирования, использования и развитие в интересах граждан, организаций, государства

Классификация угроз информационной безопасности

- Политические угрозы
- Экономические угрозы
- Организационно-технические угрозы

Угроза (Threat) – угрозой может быть любое лицо, объект или событие, которое, в случае реализации, может потенциально стать причиной нанесения вреда ЛВС

Политические факторы угроз информационной безопасности

- Изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира
- Информационная экспансия США и других развитых стран
- Становление новой государственности в странах СНГ
- Разрушение ранее существовавшей командно-административной системы государственного управления
- Нарушение информационных связей вследствие образования на территории бывшего СССР новых государств
- Стремление стран СНГ к более тесному сотрудничеству с зарубежными странами
- Низкая общая правовая и информационная культура в обществе

Экономические факторы угроз информационной безопасности

- Переход на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур - производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений
- Критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации
- Расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры стран СНГ

Организационно-технические факторы угроз ИБ

- Недостаточная нормативно-правовая база в сфере информационных отношений
- Слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг
- Широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств
- Рост объемов информации, передаваемой по открытым каналам связи
- Обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере

Иерархическая классификация угроз информационной безопасности (ИБ)

- Глобальные факторы угроз информационной безопасности
- Региональные факторы угроз информационной безопасности
- Локальные факторы угроз информационной безопасности

Система защиты информации (СЗИ)

- СЗИ – комплекс мероприятий, направленных на обеспечение информационной безопасности

Принципы построения СЗИ:

- Обеспечение ИБ – непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития СЗИ
- ИБ может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты
- Никакая СЗИ не обеспечивает ИБ без надлежащей подготовки пользователей и соблюдения ими всех правил защиты
- Никакую СЗИ нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации

СЗИ

На прикладном уровне обеспечивает:

- Подлинность и целостность информации
- Конфиденциальность информации и сообщений
- Надежную идентификацию объектов и субъектов, а также защиту от НСД
- Юридическую ответственность пользователей системы за формирование, передачу и принятие сообщений

На сетевом уровне обеспечивает:

- Высокоскоростное шифрование и цифровую подпись
- Шифрование пакетов (на сеансовых ключах)
- Реализацию функции причастности
- Прозрачность системы защиты информации
- Контроль доступа

Структура и функции системы информационной безопасности

Структура:

- Государственный центр безопасности информации
- Структурные подразделения по защите информации предприятий и организаций

Функции:

- Разработка и реализация стратегии обеспечения ИБ
- Оценка состояния ИБ
- Координация и контроль деятельность субъектов системы ИБ
- Организация фундаментальных и прикладных научных исследований в области ИБ
- Осуществление международного сотрудничества в сфере ИБ

Правовое обеспечение защиты информационной безопасности

- **Законопроекты России и Беларуси об информатизации и защите информации**
- **Закон РБ «Об электронном документе»**
- **Указ Президента РБ «Об утверждении концепции информационной безопасности»**
- **Уголовно-правовая защита от компьютерных преступлений**

ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

- компьютерное мошенничество
- компьютерный подлог (подделка)
- повреждение компьютерной информации или программ
- компьютерная диверсия (саботаж)
- несанкционированный доступ
- несанкционированный перехват информации
- несанкционированное производство патентованных компьютерных программ (пиратство программного обеспечения)
- несанкционированное воспроизводство топографии (чертежей)

Организационно-экономическое обеспечение защиты ИБ

Организационные методы защиты делятся на:

- Организационно-административные
- Организационно-технические

Организационно-административные методы защиты информации

- Выделение специальных защищенных помещений
- Выделение специальных ЭВМ
- Организация хранения конфиденциальной информации
- Использование программных средств, имеющих сертификат защищенности
- Организация специального делопроизводства
- Организация регламентированного доступа пользователей к работе на ЭВМ

Организационно-технические методы защиты информации

- Ограничение доступа посторонних лиц внутрь корпуса (запорные устройства или замки)
- Отключение ЭВМ от ЛВС
- Установка клавиатуры и печатающих устройств на мягкие подкладки
- Защита от побочных электромагнитных излучений
- Использование бесперебойных источников питания

Экономические методы защиты информации

- Организация финансовой защиты информационных ресурсов систем электронной обработки и передачи данных, т.е. «страхование»
- Например, предоставление системы гарантий для банков и их клиентов путем обеспечения страховой защиты банковских информационных «рисков»

Программно-техническое обеспечение защиты ИБ

Включает: физические, аппаратные, программные, аппаратно-программные, криптографические методы и средства защиты информации

Техническая защита информации подразделяется на:

- Пассивную защиту
- Активную защиту
- Комбинированную защиту

КОМПЬЮТЕРНЫЕ ВИРУСЫ

По среде обитания делятся на:

- Файловые
- Загрузочные
- Макровирусы
- Сетевые

По особенностям алгоритма работы:

- Резидентные
- Стелс-вирусы
- Полиморфик-вирусы
- Вирусы, использующие нестандартные приемы

По деструктивным возможностям:

- Безвредные
- Неопасные
- Опасные
- Очень опасные

КОМПЬЮТЕРНЫЕ ВИРУСЫ

«Вирусоподобные» программы:

- Троянские программы
- Утилиты скрытого администрирования удаленных компьютеров (в сетях)
- Intended-вирусы
- Конструкторы вирусов
- Полиморфик-генераторы

Антивирусные программы:

- Сканеры
- CRC-сканеры
- Блокировщики
- Иммунизаторы