БЕЗОПАСНОСТЬ

- *Информационная безопасность* - это состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие.

Признаки:

- 1) конфиденциальность: обеспечение доступа к информации только зарегистрированным пользователям;
- 2) целостность: обеспечение достоверности и полноты информации и методов ее обработки;
- 3) доступность: обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Угроза

- — это имеют возможность получить доступ к ресурсам и причинить вред.
- Угрозы подразделяются на: природные и физические; непреднамеренные; намеренные.

Защита от несанкциониро.ванного использования программного обеспечения. Средства защиты

- -система мер, направленных на противодействие нелегальному использованию программного обеспечения, защиту программного обеспечения от несанкционированного приобретения, использования, распространения, модифицирования, изучения и воссоздания аналогов. При защите могут применяться организационные, правовые, программные и программно-аппаратные средства.

Механизмы защиты

- должны обеспечивать ограничение доступа субъектов к объектам: во-первых, доступ к объекту должен быть разрешен только для определенных субъектов, во-вторых, даже имеющему доступ субъекту должно быть разрешено выполнение только определенного набора операций.

Для обеспечения защиты могут применяться следующие механизмы:

- кодирование объектов
- сокрытие местоположения объектов
- инкапсуляция объектов.

Инсайдерские атаки.

- В корпоративных приложениях осуществляется работа пользователя на одном и том же компьютере, как с открытой, так и с конфиденциальной информацией. Это расширяет возможность нарушения конфиденциальности данных санкционированным пользователям, допущенным к работе в рамках выполнения своих служебных обязанностей — инсайдерами.
- Общий подход к решению задачи защиты: на основе реализации разграничительной политики доступа к ресурсам, механизмы контроля.

Внешние атаки

- — действие, связанное с несанкционированным доступом в вычислительную сеть и преднамеренным нанесением ущерба как сети в целом, так и любым ее составным частям, включая условия или результаты их функционирования.

Средства зашиты от вредоносных программ.

- Антивирусы.
- Организационные методы (направлены на то, чтобы изменить поведение пользователя)
- Технические методы (заключаются в использовании дополнительных средств защиты, которые расширяют и дополняют возможности антивирусных программ.)

Технические средства защиты информации включают пароли и средства криптографической защиты. Технические меры защиты, как правило, применяются в совокупности с административными мероприятиями.

Имеется следующая к***лассификация средств защиты информации***:

- средства защиты от несанкционированного доступа: средства авторизации; мандатное управление доступом; избирательное управление доступом; управление доступом на основе ролей; журналирование (также называется «аудит»);
- системы анализа и моделирования информационных потоков (CASE-системы);
- системы мониторинга сетей: системы обнаружения и предотвращения вторжений (IDS/IPS), анализаторы протоколов, антивирусные средства, межсетевые экраны;
- криптографические средства: шифрование, цифровая подпись;
- системы резервного копирования;
- системы бесперебойного питания: источники бесперебойного питания; резервирование нагрузки; генераторы напряжения;
- системы аутентификации: пароль; сертификат; биометрия;
- средства предотвращения взлома корпусов и краж оборудования;
- средства контроля доступа в помещения;
- инструментальные средства анализа систем защиты: мониторинговый программный продукт.