МБУ ДО «Дом творчества» Вектор
Творческое объединение «В мире ИТ»

СПОСОБЫ ЗАЩИТЫ И ИНФОРМАЦИ И В ИНТЕРНЕТЕ

Презентация подготовлена для конкурса "Интернешка"

Комиссаров Кирилл, 11 лет
руководитель:
Ростемберская О.А.,
педагог дополнительного образования

Новокузнецк
2016

Обеспечение системы целостности информации и информационных систем

Любая информационная система, содержит следующие серверные компоненты:

шлюз-сервер, управляющий правами доступа к информационной системе;

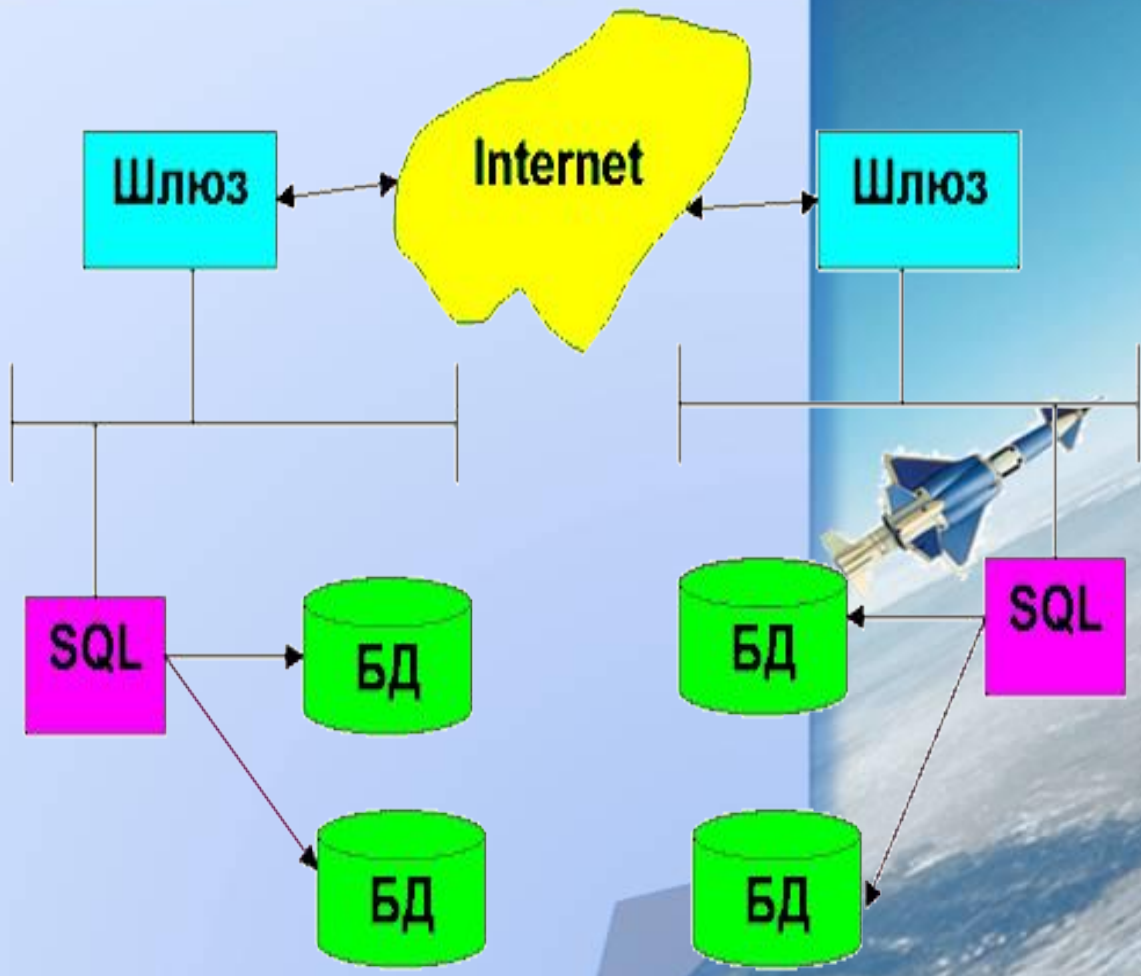
WWW-сервер;

сервер баз данных;

сервер приложений и(или) сервер обработки транзакций.

При этом среди мероприятий по защите информационных систем можно выделить три основных:

- организация системы защиты на уровне IP пакетов



Обеспечение системы целостности информации и информационных систем

Административный уровень защиты - контекстная проверка и просмотр пакетов с целью принятия решения.

Программный уровень защиты. Шлюз выступает в качестве промежуточного звена между Информационной системой и клиентом.

В случае размещения информационной системы на разных машинах, находящихся в различных локальных сетях, необходимо строить доверительные базы с обязательным применением шлюзов для обеспечения прав доступа.

Обеспечение системы целостности информации и информационных систем

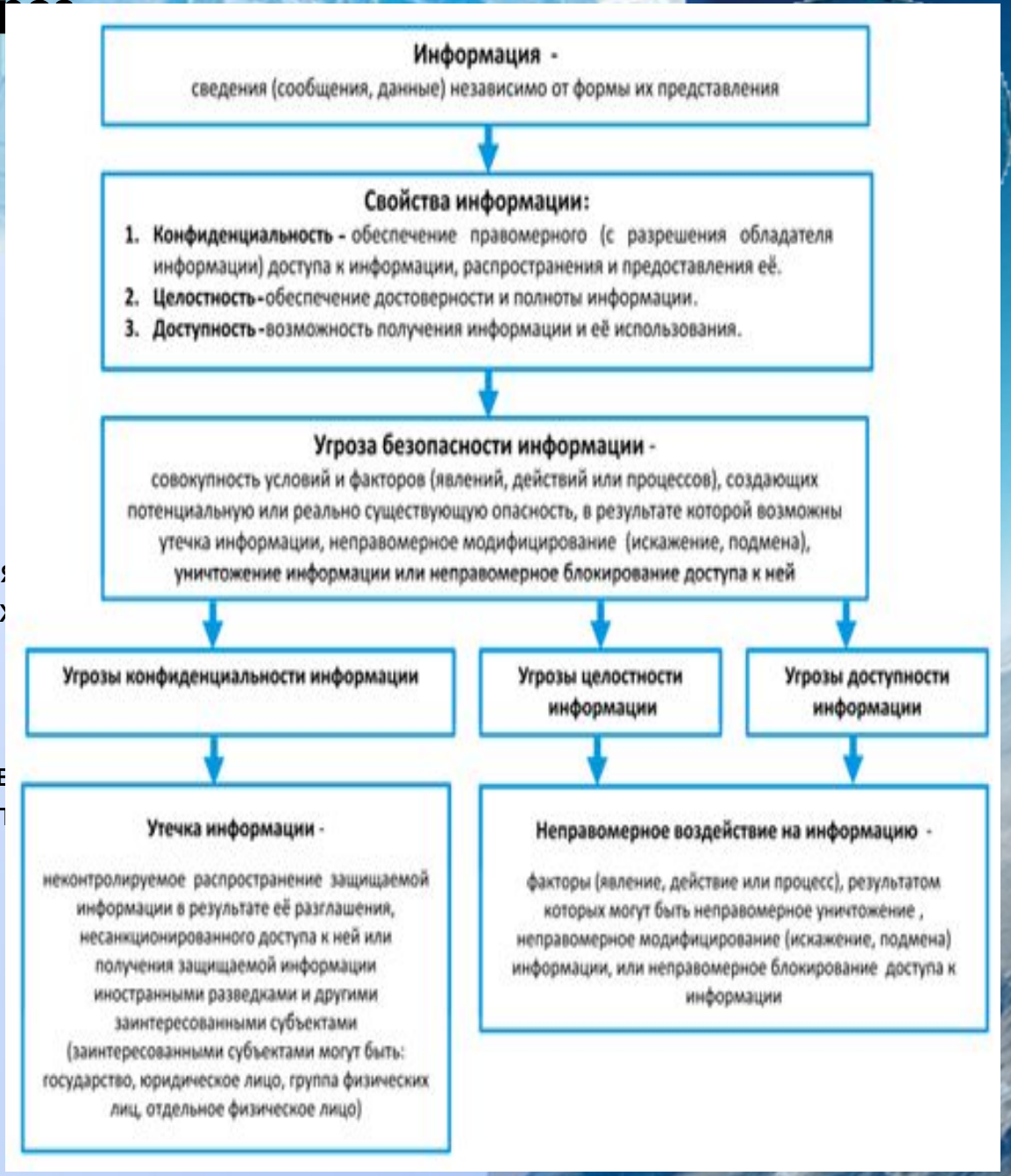
МЕТОДЫ ШИФРОВАНИЯ ДАННЫХ

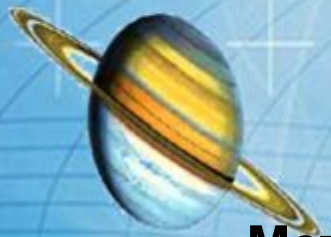
Шифрование - это способ повышения безопасности сообщения или файла, при котором их содержимое преобразуется так, что оно может быть прочитано только пользователем, обладающим соответствующим ключом шифрования для расшифровки содержимого. Например, при совершении покупки в Интернете данные сделки (такие как адрес, телефон, номер кредитной карты) обычно зашифровываются в целях безопасности. Используйте шифрование, когда требуется повышенный уровень защиты данных.

Метод шифрования называется симметричным, если для прямой и обратной процедур используется один и тот же ключ. Метод шифрования называется асимметричным, если ключ, используемый для шифрования текста отличается от другого ключа, используемого для расшифрования текста.

Классификации угроз

- Внедрение вирусов и других разрушающих программных воздействий;
- Анализ и модификация/уничтожение установленного программного обеспечения;
- Внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений;
- Использование уязвимостей ПО для взлома программной защиты с целью получения несанкционированных прав чтения, копирования, модификации или уничтожения информационных ресурсов, а также нарушения их доступности;
- Раскрытие, перехват и хищение секретных кодов и паролей;
- Чтение остаточной информации в памяти компьютеров и на внешних носителях;
- Блокирование работы пользователей



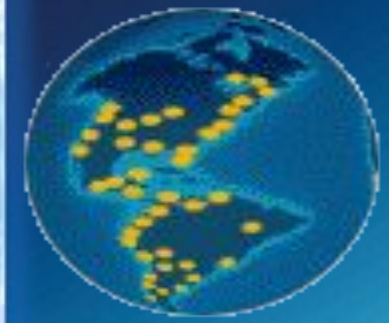


Способы несанкционированного доступа :
физический,
программно-аппаратный,
программный.

Методы обеспечения информационной безопасности

Традиционные средства защиты (антивирусы, фаерволы и т.д.) на сегодняшний день не способны эффективно противостоять современным киберпреступникам. Для защиты информационной системы организации требуется комплексный подход, сочетающий несколько рубежей защиты с применением разных технологий безопасности.

Для защиты от внешних интернет угроз информационной безопасности отлично зарекомендовали себя системы предотвращения вторжений на уровне хоста (HIPS). Правильно настроенная система даёт беспрецедентный уровень защищённости, близкий к 100%. Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации (например, антивирусного пакета) предоставляют очень высокий уровень безопасности. Это позволяет получить защиту практически от всех типов вредоносного ПО, значительно затрудняет работу хакера, решившего попробовать пробить информационную защиту, сохраняет интеллектуальную собственность и важные данные.



Источник шаблона:

Поташинская Марина Викторовна

учитель-логопед

МБОУ ШИ №133

Г. Новосибирска

Сайт:

http://pedsovet.su/

Информация:

http://www.safensoft.ru/security.phtml?c=791

http://www.intuit.ru/studies/courses/2291/591/lecture/12687

http://www.bnti.ru/showart.asp?aid=955&lvl=04.03.