

ЗАЩИТА СОБСТВЕННОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

Презентацию
подготовила:
Аристова Екатерина
Ученица 10 класса

Презентация подготовлена для конкурса:»Интернешка»

<http://interneshka.org/>

Актуальность

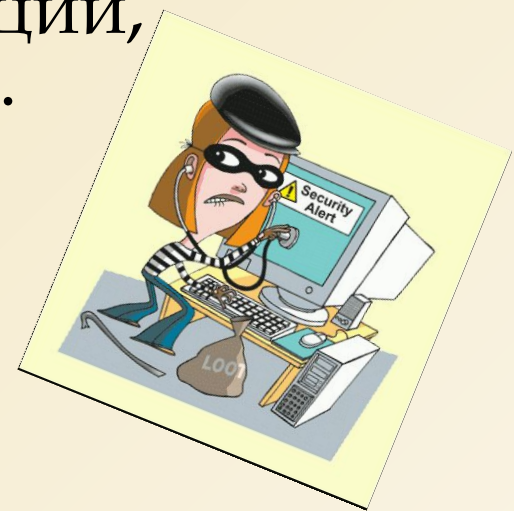
Эта тема особенно актуальна сегодня во время быстрого развития компьютерных технологий. Из-за хищения конфиденциальных данных многие компании и частные лица несут большие потери и убытки.

Определение

Несанкционированный доступ – чтение, обновление или разрушение информации при отсутствии на это соответствующих



Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи.



Цели злоумышленников

- использование компьютера для взлома других компьютеров, атак на сайты, рассылки спама, подбора паролей
- кража секретной информации — данных о банковских картах, паролей
- мошенничество (хищение путём обмана) – «нигерийские» письма (хищение денег) – «фишинг» (выманивание паролей через подставные сайты) – блокировка с требованием SMS

Несанкционированный доступ (НСД) злоумышленника на компьютер опасен не только возможностью прочтения и/или модификации обрабатываемых электронных документов, но и возможностью внедрения злоумышленником управляемой программной закладки, которая позволит ему предпринимать следующие действия:

- Читать и/или модифицировать электронные документы, которые в дальнейшем будут храниться или редактироваться на компьютере
- Осуществлять перехват различной ключевой информации, используемой для защиты электронных документов.
- Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
- Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.
- Использовать захваченный компьютер в качестве плацдарма для захвата других компьютеров локальной сети.
- Уничтожить хранящуюся на компьютере информацию или вывести компьютер из строя путем запуска вредоносного программного обеспечения.

Пути несанкционированного доступа

Перечислим основные типовые пути несанкционированного получения информации:

хищение носителей информации и производственных отходов;

копирование носителей информации с преодолением мер защиты;

маскировка под зарегистрированного пользователя;

мистификация (маскировка под запросы системы);

использование недостатков операционных систем и языков

программирования, использование программных закладок и программных блоков типа "троянский конь";

перехват электронных излучений;

перехват акустических излучений;

дистанционное фотографирование;

применение подслушивающих устройств;

злоумышленный вывод из строя механизмов защиты и т.д.

Для защиты информации от несанкционированного доступа

Применяются:

организационные мероприятия;

технические средства;

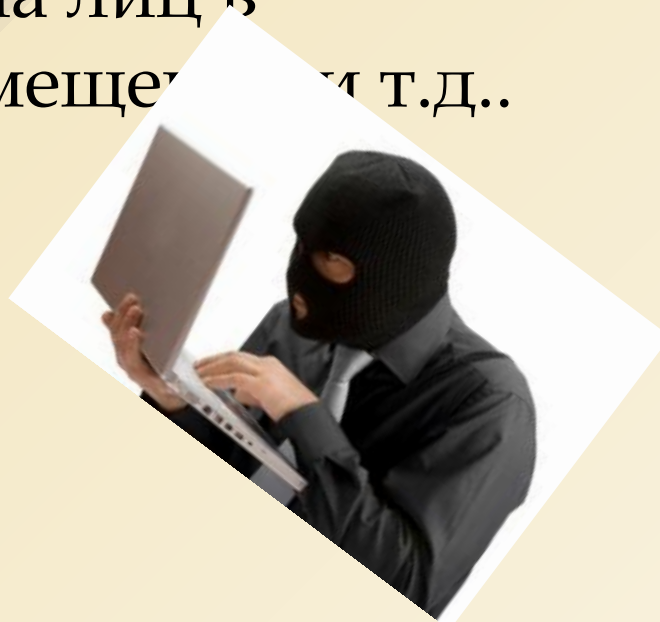
программные средства;

шифрование.

Организационные мероприятия

Включают в себя:

- пропускной режим;
- хранение носителей и устройств в сейфе (дискеты, монитор, клавиатура и т.д.);
- ограничение доступа лиц в компьютерные помещения и т.д..



Технические средства

Включают в себя:

- фильтры, экраны на аппаратуру;
- ключ для блокировки клавиатуры;
- устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати и т.д.;
- электронные ключи на микросхемах и т.д.



Программные средства

Включают в себя:

- парольный доступ – задание полномочий пользователя;
- блокировка экрана и клавиатуры с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilities;
- использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т.д.



Шифрование

Это преобразование открытой информации в зашифрованную, не доступную для понимания посторонних. Шифрование применяется в первую очередь для передачи секретной информации по незащищенным каналам связи. Шифровать можно любую информацию — тексты, рисунки, звук, базы данных и т.д. Человечество применяет шифрование с того момента, как появилась секретная информация, которую нужно было скрыть от врагов. Методы шифрования и расшифровывания сообщения изучает наука *криптология*, история которой насчитывает около четырех тысяч лет.



Правила личной безопасности

не работать с правами администратора

не запоминать пароли в браузере

использовать флажок «Чужой компьютер»
~~но использовать стандартные~~

секретные вопросы (любимое блюдо, девичья фамилия матери и т.

не размещать информацию, которая может повредить

шифровать данные (архив с) паролем

денежные операции – по протоколу HTTPS (Hypertext Transfer Protocol Secure)

Используемый материал

- ▣ <http://life-prog/ru/>
- ▣ <http://wikipedia.org/>