* Защита собственной информации от несанкционированного доступа.

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

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.

· хищение носителей информации и производственных отходов;

· копирование носителей информации с преодолением мер защиты;

· маскировка под зарегистрированного пользователя;

· использование недостатков операционных систем и языков программирования;

· использование программных закладок и программных блоков типа "троянский конь";

· перехват электронных излучений;

· дистанционное фотографирование;

· применение подслушивающих устройств;

· злоумышленный вывод из строя механизмов защиты и т.д..

* **Перечислим основные типовые пути несанкционированного получения информации:**

Средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

1) организационные мероприятия;
2) технические средства;
3) программные средства;
4) щифрование.

ционированного
а применяются:

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 Utilites;

· использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т. д.


Password
Enter the password:
****
OK
Cancel

*

Комбинированием средств защиты можно добиться относительно хорошей защищенности информации.

Не существует никаких «абсолютно надежных» методов защиты информации, гарантирующих полную невозможность получения несанкционированного доступа.

Поэтому при проектировании системы защиты от несанкционированного доступа следует исходить из предположения, что рано или поздно эта защита окажется снятой.

Спасибо за внимание!

* "Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/"