ЗАЩИТА СОБСТВЕННОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Работу выполнила
Ученица 10 «Б» класса
ГБОУ СОШ им. Е. М. Зеленова
п.г.т. Новосемейкино
Красноярского района
Самарской области
Никулина Елена

Проблема защиты информации от постороннего доступа возникла с той поры, когда человеку по каким-либо причинам не хотелось делиться ею ни с кем или не с каждым.

В следствии развития передовых технологий с каждым днем все больше и больше внимания уделяется вопросу защиты информации.

Существует притча о самом надежном способе хранения информации: «*Информация должна быть в одном экземпляре на компьютере, который находится в бронированном сейфе,* ***отключенный от всех сетей и обесточенный***».

Удобно ли работать с такой информацией? *Конечно, нет.*

В то же время пользователям необходимо защищать свои программы и данные от несанкционированного доступа (НСД).

А чтобы разрешить доступ к информации санкционированным пользователям, нужно определить, кому что можно, а что нельзя, т.е. разграничить права пользователей.

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

Для защиты информации от несанкционированного доступа применяются:

- организационные мероприятия;
- технические средства;
- программные средства;
- шифрование.

Организационные мероприятия включают в себя :

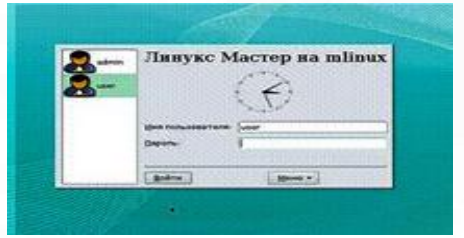
- разработка административных руководящих документов;
- пропускной режим;
- хранение носителей и устройств в сейфе (дискеты, монитор, клавиатура и т.д.);
- ограничение доступа лиц в компьютерные помещения.

Технические средства включают в себя :

- фильтры, экраны на аппаратуру;
- ключ для блокировки клавиатуры;
- устройства аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза;
- электронные ключи на микросхемах.
- резервное копирование архивов информации на жесткие диски.

Программные средства включают в себя :

- парольный доступ – задание полномочий пользователя;



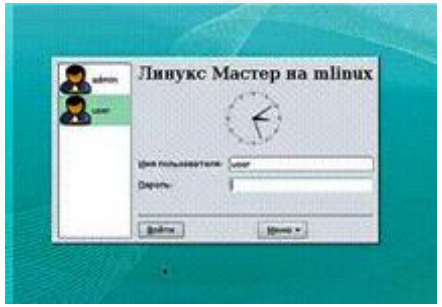
- блокировка экрана и клавиатуры с помощью комбинации клавиш в утилите **Diskreet** из пакета **Norton Utilites**;
- использование средств парольной защиты BIOS – на сам BIOS и на ПК в целом и т.д.;

- Использование современных антивирусных программ, сетевых экранов (***firewall-программа для контроля и фильтрации проходящих через него сетевых пакетов по заданным правилам.***).

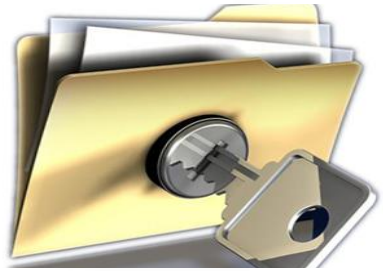
Парольный доступ используется :

- для входя в систему;

- ***идентификация*** *– пользователь сообщает системе по ее запросу свое имя (идентификатор);*
- ***аутентификация*** *- пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль);*



- для доступа к разрешенным ему программам, папкам, файлам.



В настоящее время для доступа к информации все чаще используют биометрические системы идентификации :

- идентификация по отпечаткам пальцев;
- системы распознавания речи;
- системы идентификации по радужной оболочке глаза;
- системы идентификации по изображению лица;
- системы идентификации по геометрии ладони руки.

Для защиты информации во внешнем канале связи используются следующие устройства:

- скремблеры для защиты речевой информации;

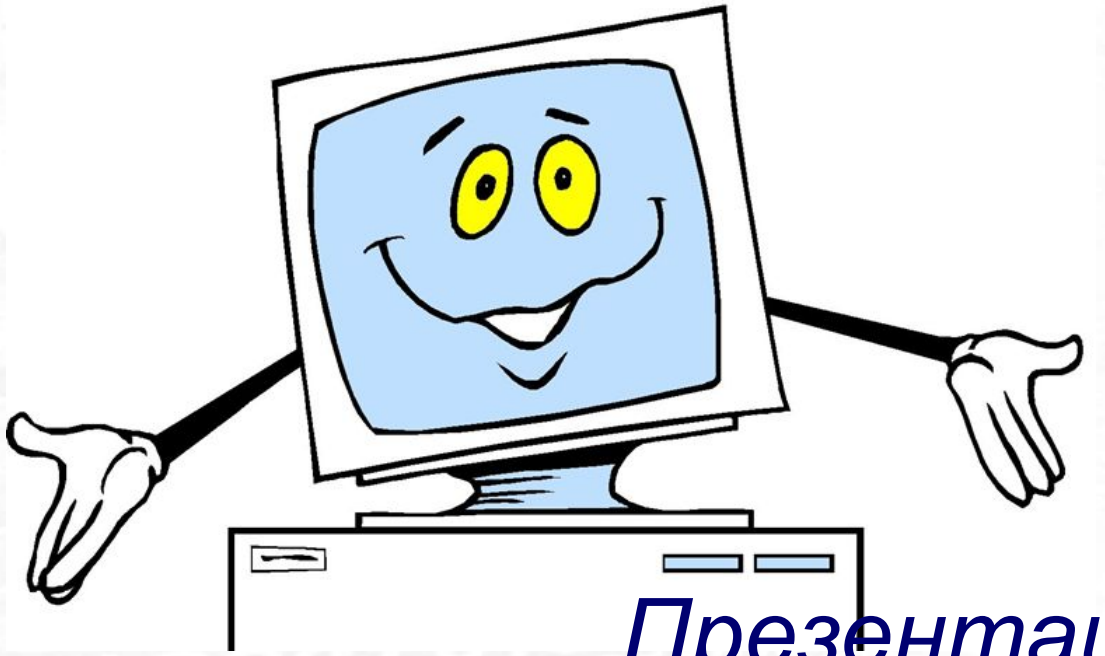
- шифраторы для широковещательной связи;

- криптографические средства, обеспечивающие шифрование цифровых данных.

В заключении можно сказать, что на данный момент с развитием технологий существует большое количество угроз, направленных на несанкциони-рованный доступ к информации и ,естественно, возникает потребность её защитить.

Главное при определении мер и принципов защиты информации - это квалифицированно определить границы разумной безопасности и затрат на средства защиты с одной стороны и поддержания системы в работоспособном состоянии и приемлемого риска с другой.

Спасибо за внимание!



Презентация подготовлена

для конкурса «Интернешка»

http://interneshka.org/