Повечето пароли имат многомилиардни комбинации и изглежда, че защита с използване на пароли е извънредно безопасен метод за охрана на системата от несанкциониран достъп. За съжаление това не е така. Опитът показва, че в типичната система, където на потребителите е разрешено да създават собствени пароли, повече от половината от избраните от тях пароли е лесно да се познаят или разшифроват.

Например в банкоматите се използват само цифри от 0 до 9, което дава 10 000 възможни комбинации. За защита на касовия апарат това е достатъчно, но не е достатъчно ако става дума за комютър, който иска да открие паролата по директния метод, когато се проверяват всички възможни комбинации от пароли, докато паролата се открие. При дълга парола (или ключ) сложността на "директното попадение" е много по-голяма.

За да се сведе до минимум успешният прехват на паролите при техния избор, е необходимо се използват различни способи:

* ограничаване броя на опитите за въвеждане на парола;
* честа смяна на паролите;
* система с две или повече пароли;
* минимална дължина на паролите;
* локаут на потребителя;
* автоматично генериране на пароли.

1. Да не се използват лични имена.

2. Да не се изписват лични имена отзад напред.

3. Да не се използва лична информация (ЕГН, номер на социална застраховка, номер на телефона, псевдоними).

4. Да не се използва професионален жаргон.

5. Да се избягват повторенията.

6. Да не се използват реални думи.

Дължината на паролата влияе съществено върху нивото на защитата.

Типичният речник, използван от програмата за проверка на правописа на текстове, има около 250 000 думи. Съществуват програми за разбиване на пароли, които могат да "извъртят" тези думи и да ги използват за проверка на паролата за по-малко от две минути.

Практиката е наложила следните правила при избор на пароли:

1. Да се избират дълги пароли, с най-малко шест или седем символа.

2. Да се използва горен и долен регистър и препинателни знаци.

3. Да се избират лесно запомнящи се пароли - не трябва да се оставят записани на хартия пароли.

4. Да се избира парола, която лесно се въвежда. Да не се дава възможност за откриване на паролата по движение на ръцете.

При създаването на производни пароли, трябва да се използват символи от различни

регистри и поне един препинателен знак.

Има няколко приьома, които могат да се използват и за сигурност, и удобство. Един от тях е да се използват в паролата две думи, разделени с препинателен знак. Например Yuor+lamP. Тук има четири особености, осигуряващи приемливост на този вид парола, които са:

* смесването на горен и долен регистър усложнява директното разбиване на паролите. В примера необикновеният преход към P намалява шансовете на хакера да го разгадае;
* достатъчната дължина на паролата намалява вероятността за откриването й чрез използване на всички думи от речника;
* двете обединени думи с препинателен знак могат да бъдат в речника, но като цяло тяхната комбинация затруднява разбиването й с помощта на речника;
* комбинацията от две прости думи е лесно да се запомни, даже ако те не са смислово свързани и няма начин да се записва някъде, за да я намери злоумишленикът;

Но парола от типа My: friend е недостатъчно сложна, защото това е използвана фраза и такъв вид пароли не трябва да се употребяват.

Могат да се използват и производни пароли - създаване на производна дума от дълга фраза. Например от фразата "Честит рожден ден, скъпи приятелю" може да се състави "чрд-сп" или нещо подобно. Обаче паролата WYSIWYG е неудачна, тъй като е акроним на известна фраза. Не трябва да се използват типични лични изказвания, по-които може да се разпознае паролата.

Също така могат да се използват и измислени думи - измисляне на нови собствени имена. Те не могат да бъдат намерени в речника. Единственото изискване е лесно да се запомнят.

Не трябва да се използва една и съща парола даже в продължение на една седмица.