**Использование современных методик создания паролей**

На современном этапе развития технологий создание паролей, которые тяжело подобрать вручную не достаточно. Киберпреступники используют сложные технологии. Многие пользователи не задумываются о существовании эффективных алгоритмов и специальных программ и продолжают создавать пароли ориентируясь только на возможности человека.

Если не использовать современные методики создания паролей, мошенники смогут подобрать их за несколько часов. Ниже представлена таблица отражающая время, которое займет у хакера взлом пароля методом перебора (Брутфорс) в 2022 году (hivasystems.io/password).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Количество символов в пароле | Только числа | Буквы в нижнем регистре | Буквы в нижнем и верхнем регистре | Числа и буквы в нижнем и верхнем регистре | Числа, буквы в нижнем и верхнем регистре, символы |
| 4 | Мгновенно | Мгновенно | Мгновенно | Мгновенно | Мгновенно |
| 5 | Мгновенно | Мгновенно | Мгновенно | Мгновенно | Мгновенно |
| 6 | Мгновенно | Мгновенно | Мгновенно | Мгновенно | Мгновенно |
| 7 | Мгновенно | Мгновенно | 2 секунды | 7 секунд | 31 секунда |
| 8 | Мгновенно | Мгновенно | 2 минуты | 7 минут | 39 минут |
| 9 | Мгновенно | 10 секунд | 1 час | 7 часов | 2 дня |
| 10 | Мгновенно | 4 минуты | 3 дня | 3 недели | 5 месяцев |
| 11 | Мгновенно | 2 часа | 5 месяцев | 3 года | 34 года |
| 12 | 2 секунды | 2 дня | 24 года | 200 лет | 3 тыс. лет |
| 13 | 19 секунд | 2 месяца | 1 тс. лет | 12 тыс. лет | 202 тыс. лет |
| 14 | 3 минуты | 4 года | 64 тыс. лет | 750 тыс. лет | 16 млн. лет |
| 15 | 32 минуты | 100 лет | 3 млн. лет | 46 млн. лет | 1 блн. Лет |
| 16 | 5 часов | З тыс. лет | 173 млн. лет | 3 бллн. лет | 92 бллн. Лет |
| 17 | 2 дня | 69 тыс. лет | 9 бллн. лет | 179 бллн.лет | 7 бллр.лет |
| 18 | 3 недели | 2 млн. лет | 467 бллн. лет | 11 бллр. лет | 438 бллр. лет |

Надежный барьер, мешающий злоумышленникам добраться до ваших данных – это уникальный надежный пароль. Чтобы его создать надо придерживаться следующих правил:

1. Использовать как минимум 10-12 символов.

2. Избегать простых последовательностей, например повторяющихся или идущих в подряд чисел или букв на клавиатуре («11111», «1234567», «qwerty»), распространенных слов («password1»).

3. Состав символов в пароле должен быть разнообразным. Используйте цифры, заглавные и строчные буквы, символы.

4. Не используйте очевидные замены символов, например вместо буквы «о» ноль.

5. Не используйте повторное использование паролей.

6. Используйте необычные (не связанные друг с другом по смыслу) сочетания слов.

7. Используйте правило, которое трудно разгадать компьютеру.

Например,составим пароль из 4 частей:

1 часть слово (не меньше 5 символов: Piano),

2 часть комбинация цифр (не используйте подряд идущие и повторяющиеся: 34),

3 часть – несколько букв (3 символа) из названия того сайта, на котором регистрируетесь (для регистрации на yandex.ru возьмем: yan),

4 часть – символы (пусть будет один :#)

В результате получим пароль : Piano34yan#. Части в пароле можно менять местами: 34yanPiano#, #34Pianoyan, Piano#yan34.

Главное придумать и запомнить правило.

кандидат технических наук, заведующий кафедройинформационных систем и математического моделирования **О.А. Астафурова**

кандидат технических наук, доцент кафедры информационных систем и математического моделирования **Н.А. Сальникова**