

Еще один способ придумывать и запоминать сложные пароли

Владимир Черняев

Ваш пароль составлен из спецсимволов, цифр, букв разного регистра, длина пароля не менее 10 символов, но всё же кажется не достаточно надёжным, так как его приходится набирать, сверяясь с записью? Прочтите статью, возможно, записывать пароль и не придётся.

Пароли являются средством защиты данных от несанкционированного доступа. Они актуальны как для корпоративных сетей, в которых заведомо есть важная информация, так и для домашнего компьютера, на котором может быть информация не для чужих глаз. Но при всей очевидности преимущества паролей, недостаток их в том, что человеку трудно запомнить устойчивые к взлому так называемые технические пароли.

Примечание: чтобы не возникло путаницы, русские буквы и слова будут отмечены типографскими кавычками – «...», английские буквы, слова будут выделены, а также все спецсимволы клавиатуры будут отмечены обыкновенными кавычками – “...”.

Технология взлома простых паролей, к примеру: “valentina”; “anitnelav” (“valentina” набранное в обратном направлении); “dfktyabyf” (при английской раскладке клавиатуры набирается русскими буквами «валентина»); “v_lentin_” (вместо буквы “a” используется “_”); и прочие, отработана давным-давно, и они не являются сколько-нибудь серьёзной преградой для злоумышленников.

Устойчивыми, безусловно, являются пароли вида: “h@81d^\$-24”; “n1\$s9<%k0r”; “>^/_1@tj5?th” – только запомнить их с первого взгляда вряд ли получится. Однако все три пароля имеют один секрет – большинству они знакомы с детства по считалочке: «На златом крыльце сидели царь, царевич, король, королевич...» – которая для данных паролей является «ключевой фразой» – фраза, которая помогает уверенно воспроизвести пароль по памяти. Попробую это продемонстрировать.

Итак: «На златом крыльце сидели царь, царевич, король, королевич...»

Первый вариант – “h@81d^\$-24”

- «На» – “h” (английское “Н” – графически схожа с русской «Н»), “@” очень похожа на «а».
- «Златом» – “gold” – золото, без гласного “о”, с заменой: “g” на 8 – графическое сходство, “l” (“L”) на 1 (единица). “l” (“L”) – 1 (единица) графическое сходство неоспоримо. Получаем “81d”.
- «Крыльце» – не используем.
- «Сидели» – “^” используем в противоположном смысле – указание вверх, а не вниз. Ассоциативное сходство со стрелкой указателем «вверх».
- «Царь» – “\$” – знак доллара (богатый, сейчас более актуально евро, но пока на клавиатуре этого знака нет).
- «Царевич» – “-” (минус), ещё не царь.
- «Король» – 2, второй после царя. Не вникая в таблицы о рангах, располагаем после «Царя».
- «Королевич» – 4, 1 – царь, 2 – король, 3 – царевич, 4 – королевич.

«На златом крыльце сидели царь, царевич, король, королевич» = “h@81d^\$-24”.

Второй вариант – “n1\$s9<%k0r”

- «На» – “Н” русское заменяем, на “n” английское (сходны по произношению). «а» = 1 (единица), первая буква алфавита).
- «Златом» – “\$” – знак доллара как эквивалент золота.
- «Крыльце» – не используем.
- «Сидели» – “s”, первая буква «С» – русская заменена на английскую – “s”. Сходна по произношению.
- «Царь» – 9, самая большая по значению цифра единиц.

- «Царевич» – “<”, близкий царю (указатель «кому близок»).
- «Король» – “%”, от величины царя.
- «Королевич» – “k0r”, первые три символа, “O” заменено, на 0 (ноль). “O” – 0 (ноль) графическое сходство.

«На златом крыльце сидели царь, царевич, король, королевич» = “n1\$9<%k0r”.

Третий вариант – “>^/_1@tj5?th”

- «На» – “>” (указание, «где» – «на», как вариант “<”).
- «Златом» – “zlat”, первые четыре символа по-английски с заменой: “z” на “^/_” – графическое сходство и “1” (“L”) на 1 («единицу») также графическое сходство.
- «Крыльце» – не используем.
- «Сидели» – “j”, похожа на присевшего человека.
- «Царь» – 5 баллов (высшая оценка).
- «Царевич» – “?”, вопрос – будет ли царём.
- «Король» – “t”, первая буква английского слова “Two” – второй после царя.
- «Королевич» – h – «Hamlet» – принц датский.

«На златом крыльце сидели царь, царевич, король, королевич» = “>^/_1@tj5?th”.

Три варианта здесь приведены для того, чтобы доказать, что даже при использовании одной и той же ключевой фразы возможно получить несхожие технические пароли. Возможно, вы попытаете воспроизвести пароли по памяти. Не получается? На практике по одной и той же ключевой фразе несколько вариантов вырабатывать нельзя. Пароль не будет воспроизведён с безусловной точностью! Сначала выбирается ключевая фраза, и потом идёт построение единственного варианта пароля.

Способы и методы, применяемые при создании технического пароля при обработке ключевой фразы

- Поворот (мысленно) символа на некий угол (обычно 90-180-270 градусов). “V” – поворот 90° – “<”, 180° – “^”, 270° – “>”.
- Зеркальное отражение, по вертикали либо по горизонтали. “e”|9 (“l” – здесь как зеркало).
- Ассоциации, вызываемые у вас, предположим с каким-то числом, именем, символом, причём ассоциации бывают, как и общеупотребительные, так и личностные – последние предпочтительней. “*” – снежинка, солнце, ежик, репей. “*” – «взрыв» – «бах», как иногда говорят. А если сменить первую букву на заглавную? Получим фамилию композитора – «Бах».
- Удвоение символа иногда даёт интересные результаты “^” + “^” = “^^” – летучая мышь, птица, корона, корона пальмы. Поворот на 90° даст возможность заменить цифру 3, букву «З». 180° – “W”. 270° – “E”. Или “{” = 0, “O”. При некотором допущении 8.
- Графическое сходство написания в алфавитах разных языков. «a» – “a”.
- Применение нескольких символов, отображающих графическое сходство с символом. «И» как “|/|”, “1/1”, “1/|”. «Я» как “9|”, “9|”,

- Сходные по звучанию. «C» – “S”. «Б» – “B”.
- Применение аналогов и синонимов слов из различных языков. «Собака» – “dog” (англ.), “Hund” (нем.), “canus” (лат.). Можно применять и антонимы – “Dog” → “Cat”.
- Графическое сходство символа с каким-либо объектом. “~” – «волна», отсюда «звук», «вода», «волнение». “~” – «дым», «неровная дорога», «змея». “&” – «узел», «змея», «лабиринт».
- Если в пароле допустимо применение букв другого алфавита – обязательно используйте это.
- Для повышения устойчивости к взлому можно добавлять несколько символов, которые вы определите сами (может быть и слово, тогда желательно разбить его на две части и внести, предположим, в начало и окончание пароля). Это также поможет исправить недостатки пароля, например в первом варианте – “h@81d^\$-24” всего две буквы. Для большей устойчивости можно добавить слово «счёт» – “schet” и внести в пароль “schh@81d^\$-24et”.

Замечание: при обработке ключевой фразы возможны любые действия со словами и символами, её составляющими. Основное, чем здесь нужно руководствоваться: ключевая фраза должна быть совершенно непредсказуема для знающих вас людей. Не быть из области вашей деятельности, увлечений и вообще того, что может быть известно тем или иным путём знающим вас людям.

Для применения в качестве ключевой фразы годится всё: марки автомобилей (разумеется, не вашего или того, о котором вы мечтаете), воспоминания детства (наиболее предпочтительны), сказки, стихи, картины, анекдоты, названия животных, природные явления – всё годится в дело.

Предположим, она из воспоминаний детства. Мысль, которая возникла во время игры в снежки. Итак:

Зима. Игра в снежки

«Получил прямо в лоб» (снежком), попробуем с ней поработать. Почему это вам запомнилось? Ну, думаю, если запомнилось – то крепко!

- «Снежок» – “*” используем второе смысловое значение слова «снежок», уменьшительно-ласкательное от «снег». Графическое сходство с падающим снежком очевидно.
- «Попал» – “->” – именно так большинство людей рисует направление движения, в данном случае полёта снежка. Желательно оставить пробел между “-” и “>”, про него вы не забудете.
- «Прямо» – у каждого имеется определённый запас иноязычных слов, которые иногда даже и неправильно связаны с русскими определениями слов. Используем английское слово “right”. Доработаем его:
 - ☑ “r” – “r”, оставляем без изменений;
 - ☑ “i” – “i”, оставляем без изменений;
 - ☑ “g” – “g”, оставляем без изменений;
 - ☑ “h” – похожа на перевёрнутую 4;
 - ☑ “t” – “t”, оставляем без изменений.
- «Лоб» – “l” – графически идеально подходит под изображение лба.

Вносим в пароль: `*->rig4t()`. Если допустимо применение букв в верхнем регистре: `*->RiG4t()`.

Пароль коротковат, посмотрим, нет ли внутренних резервов.

«Снежок» – «замерзшая» («*») вода. Запишем «вода» английскими буквами – «voda». Поработаем над этим словом:

- «v» – римское 5;
- «o» – букв у нас достаточно, попробуем перейти к графическому отображению – «[]» похоже графически;
- «d» – «d» оставляем без изменений;
- «a» – первая буква алфавита – 1 (единица) графически схожа с английской буквой «l» («L»), произведём замену 1 на «l».

Теперь вставим «замерзшая» «*» туда, куда нам заблагорассудится: `5[]d*l`.

Вносим в пароль: `5[]d*l->rig4t()`. Если допустимо применение букв в верхнем регистре: `5[]d*l->RiG4t()`.

Из личного опыта

В той или иной мере каждый из нас создаёт документы, так вот при присвоении имени документу советую писать русские слова английскими буквами. Также весьма полезны смешанные фразы, то есть использовать эквивалентное английское слово взамен русского. Например, мы создали новый документ «Чай. Его история. Виды чая». Попробуем переименовать его, как указывалось выше. У меня получилось – «Tea_Ego_history_Vidy_Chaya». Зачем это надо? Такая практика помогает при работе с ключевой фразой. Следовать этому совету или нет – личное дело каждого.

Также, если вы хотите упаковать файл и поставить пароль – само название можно преобразовать в пароль (нежелательно, если документ конфиденциален) либо (предпочтительней) использовать для выбора ключевой фразы по ассоциации, которая у вас связана со словом «чай» или, может быть, со словом «история».

Пример, иллюстрирующий преобразование названия документа в ключевую фразу, связанную со словом «история»:

«1000 лет Крещению Руси»

- «1000» – $(c+l+c+l)*3+x.x$ – «c» – римское число 100; «l» («L») – римское число 50. Второе число 50 можно записать как «vo» – «v» римское 5, «o» = 0 (ноль); «+» – сложение; «&» – как предлог «and» заменяет в данном случае знак «+»; «x» – римское число 10; «.» – заменяет знак умножения «*» – получаем математическое выражение: $(100 + 50 + 100 + 50) * 3 + 10 * 10 = 1000$.
- «л» – «l» (единица) графическое сходство с «I» («L»).
- «е» – 6 – зеркальное отображение по горизонтали (e₆).
- «т» – «t».
- «Крещению» – «-l-» – символизирует крест.
- « » «space» – «пробел» – оставляем без изменений.
- «Р» – «l0» – составной символ – графическое сходство.
- «у» – «y» – графическое сходство.
- «с» – «s» – «\$» – графическое сходство.
- «и» – «u» – графическое сходство.

«1000 лет Крещению Руси» = $(c+l+c+vo)*3+x.x16t-l-l0yu . Если допустимо применение букв в верхнем регистре: $(C+l+c+vo)*3+x.X16t-l-l0yu .

Замечание: правила применения букв верхнего регистра здесь очевидны. Первая и последняя буква в математическом выражении, которым заменили число 1000.

Иногда можно попробовать составить пароль и из сферы чьей-то, предположим, торговой деятельности с ограничениями, приведёнными выше. Попробуем разработать такой пароль из случайно услышанной фразы.

«Четверть от товара реализовали!»

- «четверть» – «0,25», «1/4».
- «от» – «>» – указатель «от чего».
- «т» – «t».
- «о» – «()» – «(» + «)».
- «в» – «[]».
- «а» – «A» = «fl» – («f» + «l»).
- «р» – «равно» – заменяем математическим символом «=».
- «а» – «ol» – графическое сходство.
- «реализовали» – «1/4>\$» – за четвертую часть получили деньги.
- «!» – «!» – оставляем без изменений.

«Четверть от товара реализовали!» = «0,25>t()[]fl=ol1/4>\$!». Если допустимо применение букв в верхнем регистре: «0,25>T()[]fl=Ol1/4>\$!». Здесь слово «товара» – «T()[]fl=Ol» – начинается и оканчивается буквами верхнего регистра.

В этом пароле интересен пример применения слова «четверть» – как в виде десятичной («0,25» – «0,25») так и простой дроби, записанной как 1/4.

Также слово «четверть» может принять ещё одно значение как ёмкость (трёхлитровая (четвертая часть округлённо от 10 литров), либо 25-литровая (четвертая часть от 100 литров) бутыл), которую можно изобразить как – «0=()» – положенная набок бутыл. «0=» – горлышко, «()» – сама ёмкость. Тогда пароль при оставлении других знаков без изменений примет такой вид: «четверть от товара реализовали!» = «0=()>t()[]fl=ol1/4>\$!».

Если вам покажется сложным этот метод – в ответ можно сказать лишь одно: оглянитесь на свой жизненный путь, что далось легко? И, право, это не самое сложное, но стоящее усилий по защите уже имеющегося. Выгода всех предложенных здесь методов – пароль можно менять так часто, как это требуется.

Пароль из картины «Три богатыря»

По порядку, точно как на картине, кто как расположен и кто, с каким оружием, не помню. Для меня они расположены так: «Алёша Попович, Илья Муромец, Добрыня Никитич».

«Алёша Попович» – «t}g>»

- 1 = «A» – первая буква алфавита.
- «t» – «Попович». «t» – похожа на крест, необходимая принадлежность сана. Можно также изобразить как «+», «-l-», либо «~l~» – уж больно не похож он на поповского сына в былинах – озорник и охальник...

- “}” либо “{” – похоже на «**лук**». Оружие Алёши.
- “g” – “g” заменяет русское «г» – «**гусли**». Очень хорошо играл, говорят.
- “>” – «стрела».

«Алёша Попович»: «**лук**» – «**гусли**» – «**стрела**» = “1t}g>”.

«Илья Муромец» – “9ml8*”

- 9 – самая большая цифра первого десятка. «**Главный**», самый «**могучий**» среди них.
- “m” – “m” заменила русскую «м» – «**Муромец**».
- “l8*” – оружие Ильи «булава» – “l*”: “l” – рукоять, оголовье-шар с шипами – “*”. Заменяем на «**утреннюю звезду**»: “l” – рукоять, 8 – цепь соединяющая с шипастым шаром – “*”.

«Главный» «Муромец» «утренняя звезда» = “9ml8*”.

«Добрыня Никитич» – “+)%n%”

- “+” – добрый, положительный “+”, как усиление – “)” улыбка из «смайликов»: “+”) = добрый, открытый.
- “n” – “n” английское заменило «н» русское («**Никитич**»).
- “%” – «**меч – голова с плеч**», и так понятно, какое оружие у Добрыни.

«Добрыня» «Никитич» «меч – голова с плеч» = “+)%n%”.

Вот что у меня получилось: “1t}g>9ml8*+)%n%&^s,3c)a”.
А вот это “&^s,3c)a” откуда?

- “&” – “and”;
- “^s” – «**шлемы**»: “^” – «**шлем**», “s” в английском – при прибавлении к окончанию предмета в единственном числе делает его множественным. Отсюда «**шлемы**» – “^s”;
- 3 – «три»;
- “c)a” – «**щита**». «Щит» – “()” левая скобка заменена на “c” в силу внешней схожести. «Щит» + «a» = «**щита**». «a» – русская заменена на “a” английскую.

“&^s,3c)a” = «и» «шлемы», «три» «щита».

Двурядный пароль – анти-keylogger

Здесь имеются в виду кейлоггеры:

- **программные, на уровне драйвера/ядра**. Заменяя собой, драйвер клавиатуры загружается до запуска любого приложения более высокого уровня, что делает его трудно выявляемым;
- **аппаратные** – реализованы как отдельные миниатюрные устройства, встраиваются в любое удобное место между клавиатурой (или в корпус клавиатуры) и системным блоком.

Кейлоггеры, имеющие средства снятия скриншотов, работающие на более высоком уровне приложений, не рассматриваются, так как выявляются антивирусами безошибочно.

На всех сайтах, требующих регистрации, вам надо ввести логин и пароль. Как-то в поисках ключевой фра-

зы для какого-то сайта долго ничего не приходило в голову. Вертелось слово «оазис». На сайте была реклама тёплых стран: пальмы, солнце, улыбающиеся лица. Словом, оазис. Ну что у нас действительно связано со словом «оазис»? Пальмы... солнце... вода... неожиданно вспомнилась фраза «Солнце, воздух и вода – наши лучшие друзья!», и тут же переделал эту фразу «**Пальмы, солнце и вода – наши лучшие друзья!**» – вот и ключевая фраза! Начал с ней работать. Ну никак не получалась пальма! И тогда я пошёл вот таким путём.

(Примечание: Так как поле «Password» не отображается в явном виде, а заменяется какими-то символами – “^” например, приходится ориентироваться по полю «Login» встраивая пароль. Заменяющие символы имеют больший размер, чем символы, вводимые в поле «Login». Поэтому ниже следующие примеры для наглядности приведены к размеру для печати. В реальности пароль выглядит:

| | |
|--------|---------------|
| Имя | ^^^~og0odDry8 |
| Пароль | |

Password: 1l/v\W+M&bug – в целях наглядности пришлось отклониться от действительного пароля. “_” не нужно для выравнивания пароля.)

Login:^^^~og0odDry8
Password: 1_ l/v\W+M&bug

Итак, приступим:

- “^” “^” “^” “~”
- “1” “1” “1” – две пальмы. “1” – «единица», “l” – “L”;
- “o”
- “/ \” – солнце, испускающее лучи, так его обычно рисуют, вероятно, многие;
- “o”
- “/v\” – солнце греет воду “v” – “voda” – «вода»;
- «**наши**» – “W+M&bug” → “Women+Man & (“and”) boy u (“и”) girl”. “W+M” – взрослые, старшие по возрасту – верхний регистр;
- «**лучшие**» → «**хорошие**» → “good” → “g0od”. Возможно также любое другое преобразование – “g00d” → “8004” (“d” – 4 буква алфавита) – “g()[]d”. Всё зависит лишь от того, что для вас наиболее приемлемо – то есть запоминаемо с безусловной надёжностью;
- «**друзья**» → «**друг**» → “dryg” → “Dry8”.

А при чём здесь анти-keylogger, скажете вы? А при том, что для набора этого пароля мне пришлось набирать его по частям, переключаясь мышкой между «Login» и «Password». Продемонстрирую, как:

Login:^^
Password:

Начинаю вводить первую пальму. Так как ствол находится в поле «Password», переключаясь мышкой в «Password». То что должно получится, если бы мы видели поле «Password»:

Login:^^
Password: 1_

Ввожу «ствол» пальмы, и для того чтобы визуально это действительно было похоже на пальму, добавляю пробел “ ” перед стволом, совмещая верхнюю и нижнюю части «пальмы». “_” – подчёркивание ставлю, чтобы «пальма» стояла на «земле», а не висела в воздухе. Первая пальма есть. Щёлкаю мышкой в поле «Login» и отображаю крону второй пальмы:

```
Login:^^~
Password: 1_
```

Щёлкаю мышкой в поле «Password», ввожу «ствол» второй пальмы, также выравнивая его “ ” (пробелом) по отношению к «кроне», находящейся в поле «Login»:

```
Login:^^~
Password: 1_ l
```

Закончив с «пальмами», начинаю вводить «солнце», также переключаясь между полями:

```
Login:^^~o
Password: 1_ l/v\
```

И так пока не введу полностью и логин и пароль. Хотя keylogger и перехватывает нажатие клавиш, но вот переключение между полями «Login» и «Password» отследить не в состоянии. Вот что он снимет при наборе, таким образом, логина и пароля – “^^1_~l o/vW+M&bug0odlDry8”. Это несколько отличается от того, что действительно ввели.

```
Login:^^~o0odDry8
Password: 1_ l/v\W+M&bug
```

С тех пор неизменно пользуюсь этим методом для создания паролей, так как тут получается больше возможностей подбора сочетаний, потому что пароли получили свободу в пространстве.

Попробуем преобразовать в обычный пароль. Вот что у меня получилось:

“^^~ 1_ log0odDry8/v\W+M&bug” – сначала отображены кроны пальм, потом стволы и солнце, остаток верхней части и остаток нижней части.

Данный способ позволяет использовать в качестве ключевой фразы любую информацию с того же сайта, где требуются логин и пароль.

Для большей устойчивости к взлому при составлении пароля необходимо помнить соотношение букв, цифр и спецсимволов.

На десять символов пароля должно приходиться:

- букв английского алфавита – 4;
- цифр арабских – 2;
- спецсимволов – 4.

Если возможно применение букв в верхнем регистре, требуется пересмотреть соотношение символов в пароле. Тогда оно будет таким:

На десять символов пароля должно приходиться:

- букв англ. алфавита нижнего регистра – 3;
- букв англ. алфавита верхнего регистра – 3;
- цифр арабских – 1;
- спецсимволов – 3.

При составлении пароля для повышения устойчивости должна учитываться вероятность появления букв в тексте. Например, для русского языка она такова:

- « » (пробел) – 18%;
- «А, И» – 6%;
- «К, М» – 3%;
- «О» – 9%;
- «Т, Н» – 5%;
- «Д, П, У, Я, Ы, З» – 2%;
- «Е» – 7%;
- «С, Р, В, Л» – 4%;
- «Б, Б, Г, Ч, Й, Х, Ж, Ю, Ш» – 1%;
- «Ц, Щ, Э, Ф» – 0,25%.

Но в некоторых приведённых выше паролях, например “RB’tu)|>_1]:w^’<a4490+>”, цифр больше, чем положено! И также букв меньше, чем в выведенном соотношении для устойчивого пароля.

А почему мы, собственно, должны в точности соблюдать правила? Чтобы облегчить кому-то составление словаря для взлома? И если один пароль и будет в точности соответствовать процентному соотношению, выведенному выше то для других это вовсе не является непреложным законом! Зачем же тогда было приводить эти примерные соотношения? Учитывать при составлении пароля их надо и не злоупотреблять какими-то одними символами при коротких паролях.

Для себя я применяю такое правило: **пароль из десяти символов – как можно более точно соответствуют выведенному соотношению. Если пароль содержит значительно более десяти знаков – символы любые.**

Пароль “RB’tu)|>_1]:w^’<a4490+>” – содержит 22 символа, и сломать его в реально приемлемое время вряд ли удастся.

Некоторые замечания из личной практики:

- Нежелательно начинать с составления пароля, содержащего более семи символов.
- Вы должны уверенно воспроизвести пароль по памяти. Обязательно записывайте пароль, пока не убедитесь, что можете воспроизводить пароли на память безошибочно.
- Если не удаётся воспроизвести пароль – смените ключевую фразу, а не перерабатывайте старую.

Заключение

На стволах орудий главного калибра дредноутов «стальные короли» наносили надпись «Ultima ratio regis» – «Последний убедительный довод».

Пароль не стреляет. Он просто отказывает в доступе.

Ставит «первый убедительный довод» защиты от несанкционированного доступа к компьютеру.

Устойчивый к взлому, уверенно воспроизводимый по памяти пароль имеет полное право именоваться «Unus ratio regis» защиты информации.

Если статья помогла вам в создании устойчивого и уверенно воспроизводимого по памяти пароля – свою задачу она выполнила. В заключение замечу: практика – лучшее средство для создания стойкого пароля.

Удачи! 