ПАМЯТКА ПОЛЬЗОВАТЕЛЮ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ

Немного о паролях

Двадцать лет мы учили пользователей привыкать к сложночитаемым и коротким паролям. Но современным облачным технологиям не важно сложночитаемый пароль или нет, есть спецсимволы или нет. Остался только один фактор – длина. Столько будет длится перебор пароля в зависимости от длины:

Кол-во знаков	Кол-во вариантов	Стойкость	Время перебора
1	36	5 бит	менее секунды
2	1296	10 бит	менее секунды
3	46 656	15 бит	менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	$2{,}821\ 109\ 9 \times 10^{12}$	41 бит	11 месяцев
9	$1{,}015\ 599\ 5 \times 10^{14}$	46 бит	32 года
10	$3{,}656\ 158\ 4 \times 10^{15}$	52 бита	1 162 года
11	$1{,}316\ 217\ 0 \times 10^{17}$	58 бит	41 823 года
12	$4{,}738\ 381\ 3 \times 10^{18}$	62 бита	1 505 615 лет

Оптимальная длина пароля – 10 символов, хоть для пользователя, хоть для администратора.

Сложность пароля — мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким-либо методом, например, методом полного перебора.

Слабый пароль — пароль, который может быть легко угадан или подобран методом полного перебора.

Сильный пароль — пароль, который трудно угадать и долго подбирать методом полного перебора.

Вычислительная машина угадывает пароли не как человек и если выбирать между добавлением еще одной буквы к паролю или заменой имеющейся на спецсимвол, то эффективнее будет выбрать первый вариант.

В подавляющем большинстве информационных систем используется защита от перебора. Пароли злоумышленниками получаются либо перехватом, либо получением хеш-сумы пароля (взлом самой информационной системы) и подбор пароля на собственных вычислительных мощностях. Защита для первого варианта – использование антивирусного ПО и запрет перехода на ссылки от неизвестных отправителей полученных электронных письмах, для второго – использование пароля большой длины.

ПАМЯТКА ПОЛЬЗОВАТЕЛЮ

ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЬНОЙ ЗАЩИТЫ

Концепция парольной защиты строится на принципах персональной ответственности, конфиденциальности пароля и минимизации привилегий. Это означает, что не зависимо от системы, домена, и т.п. у каждой учетной записи должен быть один хозяин и только он знает пароль. Только при таком подходе можно требовать персональную ответственность за сохранность пароля и за действия в домене или информационной/автоматизированной системе.

Может быть такое, что у одного работника несколько учетных записей от одной автоматизированной системы. Такое может встречаться, если работник одновременно выполняет несколько ролей в системе, например: пользователь (99% времени), администратор (1% времени).

Принципы обращения с паролями и учетными данными:

– пароли или сочетание логина и пароля – конфиденциальная информация;

– относитесь к чужим учетным данным так же, как и к своим;

– не передавайте учетные данные через недоверенных посредников. Почтовые серверы mail.orb.ru и ЕИТКС пригодны для передачи конфиденциальной информации (учетных данных). Почтовые сервера иностранных компаний (Mail, Yandex, Google (gmail.com), ...) не являются доверенными для передачи конфиденциальной информации;

Рекомендации по обращению с учетными данными (паролями).

Обфускация.

Обфускация – эффективный способ сокрытия истинной информации путём добавления в неё определённым образом дополнительных символов.

Обфускацию можно использовать при записи пароля на бумажный носитель, при утрате которого нет необходимости менять пароль и сообщать руководителю подразделения и управлению по информационной безопасности.

Пример:

Исходный пароль 34DobroyeUtro56 после обфускации выглядит так: 1234Dobroye0Utro5678. Таким образом в данном случае обфускация исходного пароля заключается в добавлении пяти символов (1,2,0,7,8) на определенные позиции, известные только автору, при этом «тело» исходного пароля остается неизменным.

Обфусцированный пароль становится набором ничего не значащих символов, невозможным к применению в исходном виде. Одним из условий

успешной обфускации пароля является добавление не менее 30% дополнительных символов к имеющимся, при этом добавляемые символы не должны выделяться ни при написании, ни при визуальном анализе, а наоборот, выглядеть логическим продолжением, как в приведенном примере.

Наследование.

Данный способ сокрытия информации удобен не только для применения в работе, но и для использования в повседневной жизни.

Нельзя везде использовать один и тот же пароль, т.к при его компрометации создаётся угроза несанкционированного доступа ко всем ресурсам.Но держать в памяти все пароли от от множества сервисов, информационных систем, сайтов – невозможно. Решение есть. Наследование.

Работает это так.

1. Необходимо придумать «тело» пароля из 10+ символов.
2. Для каждого сервиса добавлять в какое-либо определенное место идентификаторы ресурса, к которому устанавливаете пароль.

Пример:

Исходное тело пароля – PrivetMedved.Пароль для доступа к сервису doc.orb.ru может выглядеть так: PrvetDOMedved, где символы «D» и «O» в середине пароля являются сокращениями от имени сервиса - Doc.Orb.ru.

По аналогии для sed.orb.lan – PrivetSOMedved.

Важный момент! Никому и ни при каких условиях НЕЛЬЗЯ сообщать «тело» пароля, а также записывать ни в электронном, ни в бумажном виде.

Два данных принципа могут значительно облегчить жизнь с большим количеством паролей и повысить информационную безопасность в целом.