УДК 00.004

Алексеев П.А., студент 1 курса,
факультет информационных технологий,
Брянский государственный технический университет,
г. Брянск, Россия

КАК ВЫБРАТЬ ХОРОШИЙ ПАРОЛЬ?

Аннотация. *В статье рассказывается о требованиях к хорошему паролю, даются советы по составлению пароля.*

Ключевые слова: *информационная безопасность, правильный пароль, метод грубой силы.*

Annotation. *The article describes the requirements for a good password, gives tips on how to compose a password.*

Keywords: *information security, correct password, brute force method.*

Как выбрать хороший пароль

Аутентификация пользователей или подтверждение их подлинного статуса обеспечивается в основном через использование парольной защиты. Пароль – это некое сочетание символов алфавита, цифр, специальных знаков, которое имеет ограничение по длине. Уже в античности существование паролей было необходимо для осуществления безопасности. С их помощью военные командиры Древнего Рима имели возможность контролировать входящих лиц на позиции своего подразделения: враг не мог проникнуть незамеченным, поскольку на входе устанавливался меняющийся каждый день пароль, который нужно было сообщить часовым. В современный период главная функция паролей, заключающаяся в охране от несанкционированного доступа, является такой же актуальной. Пароли – незаменимые составляющие информационной безопасности при использовании электронной почты,

интернет-банка, смартфонов и прочих гаджетов, которые сохраняют персональные данные своих пользователей. По этой причине взлом пользовательских паролей является одним из наиболее часто встречающихся преступлений в сети Интернет, которое оставляет далеко позади создание бот-сетей и проведение DoS-атак. Современные киберпреступники могут применить сложные технологии для того, чтобы украсть пользовательские пароли. Это важно учитывать, так как многие люди стараются придумать пароли, которые трудно отгадать человеку, но они не берут в расчет наличие специальных алгоритмов и программ, которые способны разгадывать пользовательские хитрости при декодировании паролей. Чтобы не допустить кражи ценных данных или не стать жертвой вымогателей, необходимо создать пароли, которые будут защитой от хакеров, имеющих арсенал современных средств взлома.

Политика высокоэффективного создания паролей должна быть реализована таким образом, чтобы пользователь выбрал одновременно трудновзламываемый, но легко запоминающийся пароль. Для успешной защиты учетных записей от взлома и последующих за ним противоправных действий разумно предпринять следующие меры безопасности в отношении защиты паролей.

Несмотря на развитие надежных технических защитных средств, безопасность всех информационных систем подвергается сильному влиянию человеческого фактора. По данным исследований зачастую пользователи применяют в качестве паролей информативные последовательности символов ввиду их простой запоминаемости. Информационная составляющая применяемых паролей может определяться клавиатурным расположением символов, наличием в них фрагментов слов естественных языков, и т.п. В случае создания пароля пользователем возникает специфическая угроза безопасности, которая обусловлена человеческим фактором. При автоматической генерации исключается какая-либо взаимная связь между

личностью пользователя и паролем. Случайно созданный пароль формируется на базе гигантского массива данных, и подобрать его очень сложно.

Существует два основных подхода к составлению паролей с высокой степенью надежности. Первый подход базируется на создании кодовых фраз. Он основывается на сочетании нескольких слов. Ранее довольно часто применялись редкие слова с вставкой рандомных символов в середине и подстановкой символов, например, «basketball» можно было зашифровать как «84sk37b4LL». Современные алгоритмы взлома хорошо знакомы с таким методом. Более надежные кодовые фразы должны представлять собой сочетание слов, которые не будут связаны друг с другом и расположены в бессмысленном, рандомном порядке. Иной вариант – это предложение, которое будет разбиваться на части, и они должны будут расставляться по известным лишь самому пользователю принципам. Второй подход заключается в создании цепочки случайных символов – бессистемных сочетаний символов разных видов, где будут задействованы прописные и строчные буквы, числа, символы в случайном порядке. Поскольку расстановка символов не следует определенному методу, угадать такой пароль крайне сложно. Даже специализированные программы могут затратить многие миллионы лет на взлом подобного пароля. Прежде всего не стоит использовать простые пароли, на взлом которых может уйти небольшое количество времени. Эти виды паролей применяют клавиатурные символы из следующих категорий: строчные (a–z) и прописные (A–Z) буквы, цифры (0-9) или специальная символика. Длина пароля значительно влияет на доступность его взлома. Для обеспечения безопасности паролей важное требование заключается в том, чтобы пользователь при смене своих паролей, использовал отличные пароли от предыдущих. Трудно назвать минимальную длину пароля, которая бы всех устроила, однако обычно используют от двенадцати до четырнадцати символов, а создание более длинного пароля будет еще более хорошим решением. Следует применять разные комбинации символов с

целью придания большей сложности паролю. Стоит избегать при создании пароля очевидных словарных слов или их комбинаций. Например, «elephant» или «big elephant» - очень неудачные пароли. Число вариации в случае взлома методом подбора значительно увеличится при удлинении пароля всего на пару-тройку символов, и полный перебор всех возможных комбинаций займет не часы, а несколько дней.

Регулярная смена паролей – это основное правило личной «цифровой гигиены», которым пренебрегают очень многие. Их замену желательно проводить хотя бы один раз в полгода чтобы снизить до минимума вероятность взлома учетных записей. Категорически не рекомендуется применять одинаковый пароль к разным аккаунтам. В данном случае если преступник или злоумышленник сможет подобрать ключ к одной учетной записи, то он мгновенно получает доступ ко всем прочим. Ввиду этого в особой защите нуждается главная электронная почта, поскольку при обладании доступа к ней можно потенциально получить допуск к остальным аккаунтам.

Наконец, заключительная рекомендация касается беспечности пользователей в плане хранения парольных данных. Не стоит хранить пароли на бумаге или в файлах жесткого диска из-за небезопасности. Для того, чтобы не запоминать многочисленные пароли, можно использовать специальный менеджер, который будет сохранять их в зашифрованном виде. Правда, он теоретически тоже подвержен риску и его надо будет защищать мастер-паролем и тщательно продумать условия его хранения. Важно понимать, что пароль – это лишь одно и зачастую неглавное из средств защиты. Чтобы, определить уровень защищенности данных организации могут проводить аудит информационной безопасности. Нечто подобное может сделать обычный пользователь, оценив степень соответствия безопасности паролей здравому смыслу и обозначенным в этой статье советам. При установке даже самой совершенной парольной защиты нельзя рассчитывать на

стопроцентный результат. В современный период еще нет общедоступной аналогии для аутентификации, и пароль остается самым распространенным способом защиты. Для того, чтобы не оказаться жертвой взлома, нужно не пренебрегать правилами «цифровой гигиены» и пользоваться изложенными выше рекомендациями.

Используемые источники:

1. Михаил Райтман. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета. 2017 – СТР 38-42.

2. А.М. Блинов. Информационная безопасность.2010-стр 59-64.

3. Е. Баранова, А. Бабаш. "Информационная безопасность и защита информации " - 2016 – стр. 83-87.