УДК 004.056.53 DOI: 10.18698/2541-8009-2019-02-444

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ОБУСЛОВЛЕННЫЕ НЕПРАВИЛЬНЫМ ВЫБОРОМ ПАРОЛЕЙ

Н.А. Сухорукова nbmstu@yandex.ru
SPIN-код: 4308-9150

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В настоящее время очень актуальна защита обрабатываемой в компьютерных сетях информации от взлома и хищения. Одним из наиболее распространенных способов получения несанкционированного доступа к информации является взлом паролей. В статье рассмотрены история применения паролей при защите компьютерных данных, методы их взлома и устойчивость паролей к взлому. Показано, что устойчивость пароля определяется не только его длиной, но и такими факторами, как мощность применяемого при его создании алфавита, частота смены паролей, логическая «непредсказуемость» пароля (т. е. отказ от использования часто употребляемых слов и сочетаний клавиш). Проанализированы уязвимости паролей, обусловленные неправильными действиями пользователей при создании паролей. На основе проведенного анализа сформулированы рекомендации, которые позволяют парировать угрозы информационной безопасности, вызываемые компрометацией паролей.

Ключевые слова

Защита информации, угрозы информационной безопасности, компрометация паролей, методы взлома паролей, энтропия пароля, устойчивость пароля к взлому, рейтинг паролей, выбор пароля

Поступила в редакцию 10.12.2018

Введение. Сегодня невозможно представить себе работу в Интернете без использования паролей. Ввод паролей требуется не только на компьютере, но и на всех современных устройствах: чтобы разблокировать телефон или планшет, нужно ввести пароль. Строка из нескольких цифр или букв защищает наши личные данные, деньги, интересы.

Естественно, всегда находятся злоумышленники, пытающиеся проникнуть в наше внутреннее пространство, украсть наши деньги либо получить доступ к информации ограниченного пользования. Для этого им необходимо, в первую очередь, взломать пароли доступа.

По оценкам Центробанка России, потенциальный ущерб отечественных банков от действий хакеров может составить 1,35 млрд руб. [1], в мире сумма намного больше — порядка 172 млрд долларов [2], поэтому актуальность вопросов информационной безопасности и, в частности, защиты информации с помощью паролей, возрастает.

История появления паролей. История использования паролей насчитывает много веков. Первые пароли, написанные на деревянной табличке, применялись еще в Древнем Риме, задолго до появления Google, Skype и Microsoft. Они использовались для идентификации людей, проходящих ночью через посты охраны города, чтобы отличить друга от врага. По сути, это был простой способ защиты информации.

Фернандо Корбато, широко известный как родоначальник современного компьютерного пароля, работая в Массачусетском технологическом институте, в 1960 году предложил использовать пароли для защиты компьютерных данных.

Массачусетский технологический институт разработал огромную совместимую систему распределения времени, к которой имели доступ все исследователи. Они совместно использовали общий сервер, а также один дисковый файл. Для сохранения конфиденциальности отдельных файлов была разработана концепция пароля, чтобы пользователи могли получать доступ только к своим собственным файлам в течение выделенных им четырех часов в неделю.

После того как в 1990-х годах Всемирная паутина ворвалась в общественную жизнь, все больше и больше людей начали пользоваться Интернетом на регулярной основе, создавая массу конфиденциальных данных и информации. Естественно, что в это время остро встал вопрос защиты этой информации, в том числе с использованием криптографии [3].

Криптограф Роберт Моррис-старший, работая в Bell Labs в 1970-х годах, разработал процесс хеширования, с помощью которого строка символов преобразуется в числовой код, представляющий оригинальную фразу. Это приводит к тому, что фактический пароль не нужно хранить в базе данных паролей. Хеширование было принято в ранних unix-подобных операционных системах, которые сегодня широко используются во всем мире от мобильных устройств до рабочих станций.

Сегодня могут применяться следующие способы защиты данных (либо их сочетания) [4].

1. Одноразовый пароль (*One Time Password*, OTP), действительный только для одного сеанса аутентификации. Действие одноразового пароля также может быть ограничено определенным промежутком времени. Преимущество одноразового пароля по сравнению со статическим состоит в том, что пароль невозможно использовать повторно. Таким образом, злоумышленник, перехвативший данные из успешной сессии аутентификации, не может использовать скопированный пароль для получения доступа к защищаемой информационной системе.

2. Биометрия — система распознавания людей по одной или более физическим или поведенческим чертам. В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа.

3. Технология единого входа (*Single Sign-On*) — технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации.

4. Открытый стандарт децентрализованной системы аутентификации (*OpenID*), предоставляющей пользователю возможность создать единую учетную запись для аутентификации на множестве не связанных друг с другом Интернет-ресурсов.

При этом пароль может состоять из цифр, букв, специальных знаков, графических символов и т. д.

Проблема взлома паролей обострилась в 1990-е годы, а с началом эры облачных ресурсов стала особенно актуальной. Сегодня пользователи защищают паролями, состоящими в большинстве случаев из цифр и букв, данные своих банковских карт и онлайн-банкинга, интернет-покупок, библиотеки видео и музыки. Но насколько это безопасно? Даже такие огромные компании, как eBay, Google и LinkedIn, подвергались взлому в последние годы, что тем более ставит под угрозу пароли простых пользователей.

Методы взлома паролей. В настоящее время специалисты по кибербезопасности выделяют следующие основные методы взлома паролей [5–7].

1. Простой перебор, при котором последовательно проверяется каждый возможный набор цифр, букв и конкретных символов. Может занимать, в зависимости от сложности и длины пароля, очень много времени.

2. Перебор по словарю. Этот вид атаки применяется, когда база данных с хешированными паролями скопирована с сервера. Может сочетаться с заменой букв (опечатки) или с подстановкой цифр/слов в начало или конец слова в качестве приставки или суффикса. Также используются словари, набранные в неверной раскладке клавиатуры (русские слова в английской раскладке).

3. Метод логического угадывания. Работает в системах с большим количеством пользователей. Злоумышленник пытается понять вашу логику при составлении пароля (логин + 2 символа, логин наоборот, самые распространенные пароли и т. п.) и применяет эту логику ко всем пользователям. Если пользователей много, очень скоро произойдет коллизия и пароль будет угадан.

4. Перебор по таблице хешированных паролей. Передовой метод взлома паролей, когда хеши уже сгенерированы и остается только найти в базе соответствие хеша паролю. Работает очень быстро даже на слабых машинах и не оставляет никаких шансов владельцам коротких паролей.

5. Социальная инженерия — контакт с человеком, целью которого является выведывание нужных данных. Злоумышленник звонит жертве, представляясь сотрудником ИТ-отдела, банковских служащим, сотрудником службы безопасности и т. п., и под благовидным предлогом просит назвать пароль, pin-код, номер банковской карты и другие данные для идентификации пользователя.

6. Фишинг — проведение массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих, с целью получения доступа к конфиденциальным данным пользователей — логинам, паролям, данным лицевых счетов и банковских карт.

Устойчивость паролей к взлому. Для оценки устойчивости паролей к взлому можно использовать такой показатель, как вероятность P подбора пароля в течение его срока действия, который определяется как [8, 9]

$$P = \frac{VT}{\left|A\right|^n},$$

где V — скорость подбора пароля злоумышленником; T — срок действия пароля; A — алфавит паролей; n — длина пароля.

Обычно скорость подбора паролей V и срок действия пароля T можно считать известными. Задав допустимое значение вероятности P подбора пароля в течение его срока действия, можно определить требуемую мощность пространства паролей $\left|A\right|^n$. Следовательно, на стойкость пароля в основном влияют частота смены пароля и мощность пространства паролей, которая характеризуется длиной и используемым алфавитом при составлении пароля.

В случае использования при формировании паролей генераторов псевдослучайных последовательностей сложность пароля можно оценить с использованием понятия энтропии, впервые формализованного Шенноном как мера неопределенности или непредсказуемости информации, неопределенность появления какого-либо символа алфавита [10].

Энтропия множества $U = \{u_1, u_2, ..., u_N\}$ оценивается с помощью следующего выражения [8, 9]:

$$H(U) = -\sum_{i=1}^{N} p_i \log_2 p_i,$$

где p_i — вероятность появления элемента u_i.

Если все события появлений элементов равновероятны, т. е. $p_i = \frac{1}{N}$ $\forall_i \in \overline{1, N}$, то выражение принимает вид

$$H(U) = -\sum_{i=1}^{N} p_i \log_2 p_i = -\sum_{i=1}^{N} \frac{1}{N} \log_2 \frac{1}{N} = \log_2 \frac{1}{N}.$$

В случае $U = A^*$ информационная энтропия парольной системы определяется по соотношению

$$H(A^*) = \log_2 \left|A^*\right| = \log_2 \left|A\right|^n = n \log_2 \left|A\right|.$$

Величина $H(A^*)$ характеризует степень случайности пароля при его генерации и показывает, насколько сложно его угадать злоумышленнику. Например, для известного пароля энтропия равна нулю. Если пароль имеет энтропию, равную 1 символу, то угадать его с первой попытки можно с вероятностью рав-

ной 1/*A*. Значения энтропии в расчете на один символ для различных алфавитов приведены в табл. 1.

Таблица 1

Значения энтропии в расчете на один символ для различных алфавитов

Алфавит *A*	Число символов *n*	Энтропия на один символ $\log_2\|A\|$
Арабские цифры (0–9)	10	3,3219
Шестнадцатеричные числа (0–9, A–F)	16	4,0000
Латинский алфавит (a–z, A–Z)	52	5,7004
Латинский алфавит с цифрами (a–z, A–Z, 0–9)	62	5,9542
Таблица ASCII	94	6,5546

Такой анализ методом прямого подбора применим к паролям, состоящим из случайных последовательностей букв, цифр и символов. Однако в большинстве случаев и лишь за редким исключением, пользователи выбирают в качестве пароля упорядоченные комбинации символов — словарные слова, простые клавиатурные последовательности, например qwerty, asdf и zxcvbn, повторы, последовательности, а также сочетания вышеперечисленных элементов. Если пароль содержит буквы верхнего регистра, то такой буквой, скорее всего, будет первая буква пароля. Использование цифр и специальных символов также зачастую предсказуемо, в частности благодаря использованию сетевого жаргона l33t (цифра 3 заменяет букву e, 0 — o, @ или 4-a).

Без проверки использования общеупотребительных комбинаций рекомендация использовать в пароле цифры и символы ненамного усложнит взлом, зато значительно усложнит запоминание.

Для оценки стойкости парольных систем, в которых используются генераторы псевдослучайной последовательности, могут быть использованы различные статистические тесты [11]. Генератор псевдослучайной последовательности рассматривается как программа, которая генерирует битовые последовательности вида $\overline{S} = (S_1, S_2, ..., S_n)$, $S \in \{0,1\}$. Данные последовательности подвергаются статистическим тестам, в ходе которых определяется мера их случайности. Методы тестирования описываются с использованием нулевой гипотезы H_0 (тестируемая последовательность является случайной) и альтернативной гипотезы H_1 (тестируемая последовательность не является случайной). Тест разрабатывается с целью проверки нулевой гипотезы H_0.

Процесс статистического тестирования в общем случае выглядит следующим образом:

– формулируется гипотеза H_0 — последовательность $\overline{S}$ является случайной с равномерным распределением — и противоположная ей гипотеза H_1;

– фиксируется уровень значимости α;

– задается статистика $T: \{0,1\}^n \to R$;

– для заданной последовательности $\overline{S}$ вычисляется статистика $T = T(\overline{S})$;

– вычисляется достигаемый уровень значимости $p = p(T)$ значения статистики;

Если $p \geq \alpha$, то принимается нулевая гипотеза H_0, иначе гипотеза H_0 отвергается.

Компания SplashData, занимающаяся вопросами компьютерной безопасности, опубликовала рейтинг 25 самых популярных, а следовательно, и самых раскрываемых паролей, приведенных в табл. 2. Рейтинг составлен на основе информации о похищенных и раскрытых хакерами данных.

Заметим, что длина топ-25 самых популярных паролей находилась в диапазоне от 6 до 8 знаков. При этом в 6 самых популярных паролях были только арабские цифры, в 16 — только строчные буквы латинского алфавита и лишь в трех паролях наблюдалось сочетание строчных букв с арабскими цифрами. С точки зрения взлома методом полного перебора устойчивость пароля к хакерским атакам сильно зависит как от его длины, так и от используемого набора знаков.

Таблица 2

Самые популярные пароли

№ п/п	Пароль	Уязвимость к взлому методом догадки	Количество знаков	Алфавит	Мощность	Энтропия пароля, в битах
1	password	пароль	8	Строчные латинские буквы	26	37,6
2	123456	соседние цифры	6	Арабские цифры	10	19,9
3	12345678	соседние цифры	8	Арабские цифры	10	26,6
4	qwerty	соседние буквы	6	Строчные латинские буквы	26	28,2
5	abc123	первые буквы алфавита и первые три цифры	6	Арабские цифры + строчные латинские буквы	36	31,0
6	monkey	обезьянка	6	Строчные латинские буквы	26	28,2
7	1234567	соседние цифры	7	Арабские цифры	10	23,3
8	letmein	Позвольте мне войти	7	Строчные латинские буквы	26	32,9
9	trustno1	траст № 1	8	Арабские цифры + строчные латинские буквы	36	41,4
10	dragon	дракон	6	Строчные латинские буквы	26	28,2
11	baseball	бейсбол	8	Строчные латинские буквы	26	37,6
12	111111	одна и та же цифра	6	Арабские цифры	10	19,9
13	iloveyou	я люблю тебя	8	Строчные латинские буквы	26	37,6
14	master	хозяин	6	Строчные латинские буквы	26	28,2
15	sunshine	солнечный свет	8	Строчные латинские буквы	26	37,6

Окончание табл 2

№ п/п	Пароль	Уязвимость к взлому методом догадки	Количество знаков	Алфавит	Мощность	Энтропия пароля, в битах
16	ashley	имя	6	Строчные латинские буквы	26	28,2
17	bailey	стена замка	6	Строчные латинские буквы	26	28,2
18	passw0rd	пар0ль	8	Арабские цифры + строчные латинские буквы	36	41,4
19	shadow	тень	6	Строчные латинские буквы	26	28,2
20	123123	соседние цифры	6	Арабские цифры	10	19,9
21	654321	соседние цифры	6	Арабские цифры	10	19,9
22	superman	супермен	8	Строчные латинские буквы	26	37,6
23	qazwsx	соседние цифры	6	Строчные латинские буквы	26	28,2
24	michael	имя	7	Строчные латинские буквы	26	32,9
25	football	футбол	8	Строчные латинские буквы	26	37,6

В качестве примера рассмотрим энтропию самого легкого для взлома пароля 123456. Она составит $H_{123456} = 6 \cdot \log_2 10 = 19{,}9$ бит. В то же время энтропия пароля trustno1, т. е. относительно сложного пароля из топ-25 самых популярных паролей, равна 41,4 бит. Вполне очевидно, что чем меньше сложность пароля, измеренная в битах, тем легче его взломать методом полного перебора. Однако главной ахиллесовой пятой 25 самых популярных паролей является не столько их длина и ограниченный набор символов, используемых для их составления, сколько вполне очевидная их уязвимость перед взломом, так называемым методом логического угадывания. Например, 10 паролей представляют собой часто используемые в английском языке слова, пять паролей содержат соседние цифры, два пароля — соседние буквы на клавиатуре, а еще два пароля — популярные имена.

Таким образом, энтропия пароля, сгенерированного случайным образом, для топ-25 самых популярных паролей представляется завышенной оценкой их сложности, так как не учитывает их уязвимости к взлому методом логического угадывания.

Уязвимости, обусловленные пользователем. Если веб-сайт требует регистрации, он почти наверняка использует пароли в качестве средства аутентификации пользователей. Даже различные устройства, которые в настоящее время используют биометрию для проверки подлинности, по-прежнему полагаются на главный пароль (или код доступа) в качестве резервной копии.

Проблемой является то, что большинство пользователей в ущерб безопасности выбирает простые, легко запоминающиеся последовательности символов для создания пароля. Кроме того, около 60 % пользователей используют одинаковый пароль на различных сайтах.

Многие из веб-сайтов, которые требуют от пользователей регистрации и создания защищенных паролем учетных записей, не предоставляют пользователю

каких-либо указаний для выбора пароля. Для оценки выбора они чаще всего ограничиваются счетчиками длины пароля, поэтому у пользователей нет понимания, почему пароль, который они выбрали, является слабым и как сделать его сильнее.

Конечно, многие сайты все еще применяют ограничения при выборе пароля, но даже самые популярные из них удивительно неосмотрительны. Например, Facebook запрещает использование в качестве пароля слова «пароль» или “qwerty”, но в то же время пользователи по-прежнему могут использовать в качестве пароля свою фамилию и цифру «1» после нее. Поэтому неудивительно, что пользователи продолжают делать плохой/слабый выбор.

Если пользователи склонны выбирать слабые пароли, не будут ли они делать это в любом случае, независимо от подсказок и рекомендаций сайта? Для ответа на этот вопрос был проведен эксперимент с привлечением 300 пользователей [12]. Он показал, что простое наличие указаний (т. е. перечисление правил без их принудительного применения) существенно влияет на выбор пароля. Исследование было предназначено для наблюдения за реалистичным поведением выбора пароля и оценивало пять сценариев, при этом каждый сценарий был предложен шестидесяти участникам:

1. Пароли выбирались без каких-либо указаний или комментариев вообще.

2. Рядом с полем выбора пароля были представлены четыре основных указания (а именно, что пароль должен быть не менее 8 символов длиной, должен включать как прописные, так и строчные буквы, как минимум один номер и один специальный символ; также следует избегать употребления словарных слов или личной информации).

3. Руководство было дополнено стандартным счетчиком паролей, рейтингом выбора пароля как слабого, среднего или сильного.

4. Счетчик был заменен на грустные, нейтральные и счастливые смайлики, чтобы обозначить пригодность выбора. Это было сделано, чтобы оценить, как пользователи могут ответить по-другому на что-то более эмоциональное (например, они будут прилагать больше усилий, чтобы попытаться угодить системе и получить улыбающееся лицо).

5. Выбор пароля сопровождался эмоциональным сообщением обратной связи (например, «Это недостаточно хорошо!» для слабого выбора пароля), одновременно стандартно информируя о рейтинге пароля «слабый/средний/сильный».

Результаты показали резкую разницу между неуправляемым и управляемым сценариями: слабый выбор уменьшается с 75 % в первом сценарии до примерно трети в последнем (параллельно пароли, оцененные как сильные, выросли с нуля до 12 % в результате подсказок и обратной связи). Средняя длина выбранных паролей составляла от 6,7 символов в неуправляемом сценарии до 8,8 символов в сценарии с ориентацией и эмоциональной обратной связью, при этом разнообразие символов также увеличилось.

Рекомендации по устранению угроз информационной безопасности. Анализ устойчивости паролей к взлому и уязвимостей, обусловленных легкомысленным отношением пользователей к выбору паролей, позволяет сформу-

лировать базовые рекомендации по устранению угроз информационной безопасности.

1. Большинство рекомендаций устанавливает минимальную длину пароля равной 8 символам, рекомендованную — 14 символам. Хакеры сначала проверяют самые простые и распространенные пароли, а затем уже переходят к паролям с наименьшим числом символов. В то время как пароль с семью символами может быть взломан за 0,29 миллисекунд, на взлом пароля из 12 символов может потребоваться до двух столетий.

2. Расширение алфавита паролей специальными символами или буквами в верхнем регистре повышает стойкость парольной системы.

3. Большинство документов рекомендует использовать пароли временного действия, что позволяет повысить стойкость парольной защиты. Периодически, не реже 1 раза в 90 дней, пароли необходимо менять.

4. Часто для взлома паролей используются кейлогеры — вирусные программы, отслеживающие нажатия клавиш. Использование файервола, установление менеджера паролей, который будет автоматически заполнять поля с паролями, а также регулярное обновление установленного программного обеспечения позволяет нейтрализовать кейлогеры.

5. Использование теста «вызов-ответ» (challenge-response) для предотвращения автоматической отправки на страницу входа. Такие системы, как reCAPTCHA, могут требовать ввода слова или решения математической задачи, чтобы убедиться в том, что регистрационные данные вводит человек, а не хакерская система.

6. Осторожное отношение к письмам от непонятных отправителей, игнорирование просьб подтвердить персональную или финансовую информацию или требований о немедленных действиях с помощью угрожающей информации. Не переходите по ссылкам, не скачивайте файлы или не открывайте вложения от неизвестных отправителей. Никогда не отправляйте личную или финансовую информацию по электронной почте даже тем людям, кому вы доверяете, так как ваша почта может быть взломана.

7. При выборе пароля избегайте в нем любых слов из словаря или общеизвестных и предсказуемых вариаций слов. Используйте SSH-ключи для подключения к удаленному серверу для хранения вашего пароля. Вам также следует разрешать SSH-подключения только для определенных хостов или IP-адресов, чтобы вы могли точно знать, какие компьютеры подключаются к вашему серверу.

8. Храните пароли в безопасном месте.

9. Установите антивирусную программу на все устройства, чтобы следить за подозрительной активностью и не допускать установки на ваш компьютер неизвестных программ и утилит.

Заключение. В данной статье рассмотрена история появления паролей, приведены наиболее распространенные методы взлома паролей, проанализированы устойчивость паролей к взлому и уязвимости, обусловленные пользователем.

На основе результатов анализа методов взлома, оценок устойчивости паролей и анализа основных ошибок, допускаемых пользователями, сформулированы рекомендации по парированию угроз информационной безопасности, которые могут быть вызваны компрометацией паролей.

Литература

[1] ЦБ оценил потенциальный ущерб банков от действий хакеров в 2017 году. *Rbc.ru*: веб-сайт. URL: https://www.rbc.ru/finances/16/02/2018/5a869b6c9a794738db5d10da (дата обращения 05.11.2018).

[2] Ущерб от хакеров за 2017 год оценили в 172 млрд долларов. *dailycomm.ru*: веб-сайт. URL: http://www.dailycomm.ru/m/43911/ (дата обращения 05.11.2018).

[3] A short history of the computer password. *welivesecurity.com*: веб-сайт. URL: https://www.welivesecurity.com/2017/05/04/short-history-computer-password/ (дата обращения 05.11.2018).

[4] Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. СПб., Университет ИТМО, 2014.

[5] Most common password cracking methods and their countermeasures. *techcubers.com*: веб-сайт. URL: https://techcubers.com/tips-and-tricks/6-most-common-password-cracking-methods-and-their-countermeasures/ (дата обращения 05.11.2018).

[6] Простой и надежный пароль - коллективное творчество. *habr.com*: веб-сайт. URL: https://habr.com/post/118499/ (дата обращения 07.11.2018).

[7] Что такое фишинг. *avast.ru*: веб-сайт. URL: https://www.avast.ru/c-phishing (дата обращения 10.11.2018).

[8] Количественная оценка стойкости парольной защиты. *cyberpedia.su*: веб-сайт. URL: https://cyberpedia.su/11x65b9.html (дата обращения: 10.11.2018).

[9] Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М., Академия, 2005.

[10] Тюрин К.А., Сёмин Р.В. Анализ стойкости парольных фраз на основе информационной энтропии. *Известия ЮФУ. Технические науки*, 2015, № 5(166), с. 18–27.

[11] Марков Г.А. Метрики стойкости парольной защиты. *Молодежный научно-технический вестник*, 2013, № 2. URL: http://ainsnt.ru/doc/541673.html

[12] Furnell S. The death of passwords: cybersecurity's fake new. *(In)Secure Magazine*, 2017, no. 54, pp. 10–12. URL: https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-54.pdf

Сухорукова Надежда Алексеевна — студентка кафедры «Защита информации», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

THE INFORMATION SECURITY THREATS CONDITIONED BY INCORRECT PASSWORD SELECTION

N.A. Sukhorukova
nbmstu@yandex.ru
SPIN-code: 4308-9150

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Nowadays, the protection of information, processed in computer networks against hacking and embezzlement, is very relevant. One of the most common ways to obtain unauthorized access to information, is password cracking. The article describes the history of the passwords use in the protection of computer data, methods of their hacking and the password resistance to hacking. It is shown that the password stability is determined not only by its length, but also by such factors as the power of the alphabet, used for its creation, the frequency of changing passwords, the logical "unpredictability" of a password (i.e. the rejection of the use of frequently used words and shortcuts). The password vulnerabilities due to incorrect user actions during passwords creation, were analyzed. The recommendations were formulated on the basis of this analysis, that allow to counter the threats of information security caused by password compromise.

Keywords

Information protection, information security threats, password compromise, password cracking methods, password entropy, password resistance, password rating, password selection.

Received 10.12.2018

References

[1] TsB otsenil potentsial'nyy ushcherb bankov ot deystviy khakerov v 2017 godu [Central bank estimated expected bank losses from hacker actions in 2017]. *Rbc*.ru: website (in Russ.). URL: https://www.rbc.ru/finances/16/02/2018/5a869b6c9a794738db5d10da (accessed 05.11.2018).

[2] Ushcherb ot khakerov za 2017 god otsenili v 172 mlrd dollarov [Estimated losses from hacker actions in 2017 are about 172 billion dollars]. *dailycomm.ru*: website (in Russ.). URL: http://www.dailycomm.ru/m/43911/ (accessed 05.11.2018).

[3] A short history of the computer password. *welivesecurity.com*: website. URL: https://www.welivesecurity.com/2017/05/04/short-history-computer-password/ (accessed 05.11.2018).

[4] Shcheglov A.Yu. Modeli, metody i sredstva kontrolya dostupa k resursam vychislitel'nykh system [Models, methods and means of access control to the computer systems resources]. Sankt-Petersburg, Universitet ITMO Publ., 2014 (in Russ.).

[5] Most common password cracking methods and their countermeasures. *techcubers.com*: website. URL: https://techcubers.com/tips-and-tricks/6-most-common-password-cracking-methods-and-their-countermeasures/ (accessed 05.11.2018).

[6] Prostoy i nadezhnyy parol' — kollektivnoe tvorchestvo [Simple and computer systems password: a collective art]. *habr.com*: website (in Russ.). URL: https://habr.com/post/118499/ (accessed 07.11.2018).

[7] Chto takoe fishing [What is fishing?]. *avast.ru*: website (in Russ.). URL: https://www.avast.ru/c-phishing (accessed 10.11.2018).
[8] Kolichestvennaya otsenka stoykosti parol'noy zashchity [Quantitative estimate of the password protection security]. *cyberpedia.su*: website (in Russ.). URL: https://cyberpedia.su/11x65b9.html (accessed 10.11.2018).
[9] Khorev P.B. Metody i sredstva zashchity informatsii v komp'yuternykh sistemakh [Methods and means for information protection in computer systems]. Moscow, Akademiya Publ., 2005 (in Russ.).
[10] Tyurin K.A., Sëmin R.V. Analysis of passphrases resistance based on information entropy. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, no. 5(166), pp. 18–27 (in Russ.).
[11] Markov G.A. Strength metrics of password protection. *Molodezhnyy nauchno-tekhnicheskiy vestnik*, 2013, no. 2. URL: http://ainsnt.ru/doc/541673.html (in Russ.).
[12] Furnell S. The death of passwords: cybersecurity's fake new. *(In)Secure Magazine*, 2017, no. 54, pp. 10–12. URL: https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-54.pdf

Sukhorukova N.A. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.