

УДК 004.056.5

Психологические аспекты безопасности в сети: выбор паролей

Геворгян Элен Артаковна

gevorgyaneaa1@student.bmstu.ru

Потапов Алексей Вячеславович

potapov@bmstu.ru

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

В работе рассмотрены психологические аспекты выбора паролей для учетных записей. Нежелание придумать сложный пароль, и проблема его запоминания приводит к тому, что злоумышленникам становится проще взламывать пароли и добраться до конфиденциальной информации. Цель работы — доложить об опасности выбора простых паролей из-за ассоциативного выбора слов или символов. Описаны методы выбора безопасных паролей и ее защищенности. Проведен социальный эксперимент, приведена статистика использования простых паролей и сделан вывод об осведомленности людей о незащищенности паролей.

Ключевые слова: пароль, социальная инженерия, психология выбора, угроза, опасность, незащищенность, учетная запись, взлом, безопасность, конфиденциальность

В стремительно развивающемся мире цифровых технологий важно обращать внимание не только на программные и аппаратные средства защиты информации, но и на социально-психологические аспекты. В настоящее время термин «Социальная инженерия» обретает особую значимость в сфере IT и информационной безопасности. Это искусство психологического манипулирования, которое злоумышленники используют для добычи конфиденциальной информации.

При создании аккаунтов в разных сервисах пользователи часто раскрывают свои данные: день рождения, родной город, страну проживания, учебные заведения и прочее. Разделы об интересах, любимых цитатах, мировоззрении и социальном статусе хранят информацию, которая может облегчить взлом. Публикация фотографий с геолокацией, именами домашних питомцев или местами работы создает дополнительные риски, если пароли содержат схожие ассоциации. Хакеры могут прибегать к «словарным атакам», пользоваться информацией о местонахождении для кибератаки в моменты, когда жертва отвлечена. Повторное использование паролей или одних и тех же ассоциаций для разных учетных записей лишь усугубляет эту угрозу, так как открывает доступ ко всем аккаунтам. Под угрозой могут оказаться не только личные аккаунты, но и рабочие, если не соблюдать основные правила создания надежного пароля. По исследованиям компании Trustwave более 5 % всех паролей в своей символике содержат набор password или различные его вариации, для бизнес- и коммерческих аккаунтов такая ошибка может оказаться колоссальной [1, 2].

Надежный пароль характеризуется тяжестью взлома, чем дольше происходит подбор пароля, тем он сложнее. Если не пользоваться современными

методиками создания паролей, то вероятно, что мошенники смогут подобрать их буквально за несколько часов.

Критерии надежного пароля:

- более 10–15 символов;
- отсутствие простых и известных последовательностей, например “12345” / “11111” или “qwerty” / “password”;
- разнообразный состав символов (строчные/заглавные буквы, алфавиты разных языков, цифры и знаки).

Для лучшей надежности можно прибегнуть к помощи генераторов паролей. С помощью менеджера паролей нет необходимости запоминать последовательность, следовательно проблема запоминания тоже решена [3, 4].

В связи острой проблемой взлома паролей и неосведомленности граждан был проведен социальный эксперимент на тему: выбор паролей, в котором приняли участие 120 человек, отражающий знания о паролях и методы выбора.

Вопросы, на которые отвечали участники:

Как часто вы используете ассоциации (имена, названия, числа) при создании логинов и паролей для онлайн-сервисов?

Какими типами ассоциаций вы чаще всего пользуетесь?

Как бы вы оценили уровень безопасности использования ассоциаций для создания паролей? (Шкала от 1 до 5, где 1 — «очень небезопасно», 5 — «очень»).

Сталкивались ли вы с ситуацией, когда ваш пароль, созданный с использованием ассоциаций, был взломан?

Как вы обычно создаете пароли, если не используете ассоциации?

Изменяете ли вы свои пароли регулярно?

Используете ли вы одинаковые пароли для разных онлайн-сервисов?

Работаете/учитесь ли Вы в сфере IT?

Алан Браун в своей работе «Генерация и запоминание паролей» раскрывает результаты исследования, в котором выясняется, что имена являются наиболее распространенной информацией, используемой для паролей, а даты являются вторым по распространенности типом информации [5].

По результатам проведенного опроса в были сделаны выводы. Практически 70 % участников ответили, что иногда или часто используют ассоциации. На первом месте использование имен и на втором — ключевые даты. Исследование подтвердило эксперимент Алана Брауна.

Пароли, созданные с помощью ассоциаций, безопасны на «5» и «4» баллов по мнению 60 % опрошенных. Пароли стоит обновлять периодически. Многие IT-компании в политике безопасности указывают, что изменение паролей раз в единицу времени — обязательная процедура, рабочие аккаунты могут оказаться под угрозой, если не соблюдать политику паролей, установленной предприятием. Необходимо использовать разные пароли для разных сервисов, чтобы злоумышленники не смогли получить доступ ко всем аккаунтам.

В работе была подсчитана корреляция частоты использования ассоциаций в паролях в зависимости, работает/учится ли участник опроса в сфере ИТ. Корреляция = 0,3, она положительна, следовательно при повышении одного значения частоты вырастают и другие значения.

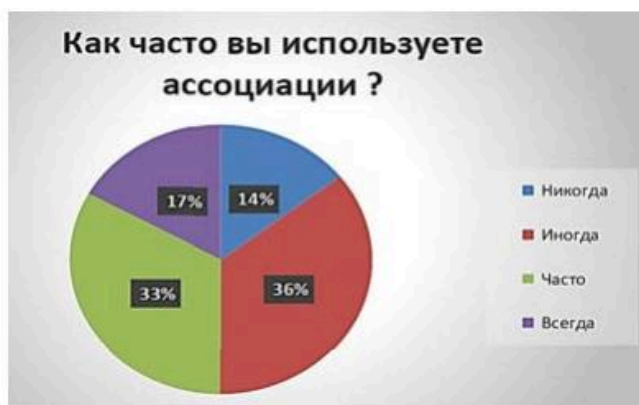


Рис. 1. Частота пользования ассоциациями

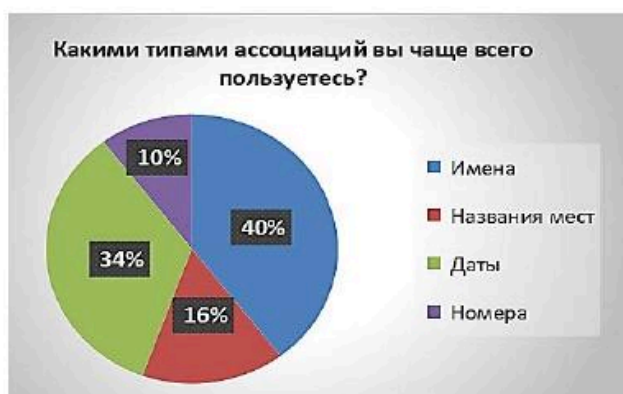


Рис. 2. Часто используемые ассоциации

Как бы вы оценили уровень безопасности использования ассоциаций для создания паролей? (Шкала от 1 до 5)

1 2 3 4 5

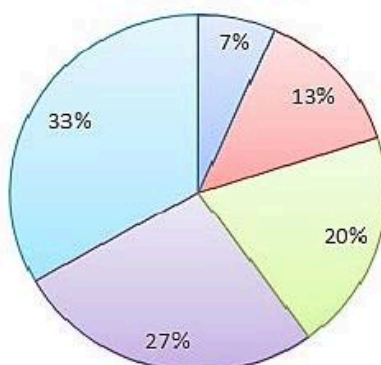


Рис. 3. Оценка безопасности пароля с ассоциацией

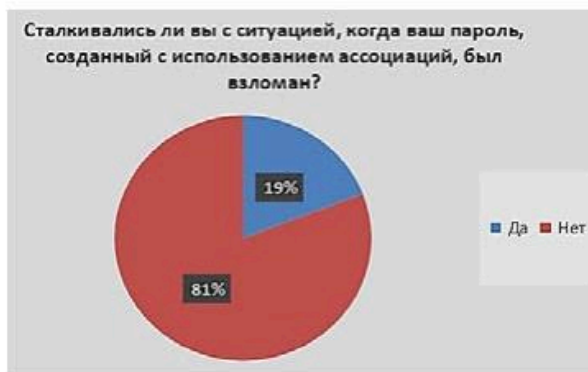


Рис. 4. Частота взлома паролей с использованием ассоциаций



Рис. 5. Использование альтернатив создания

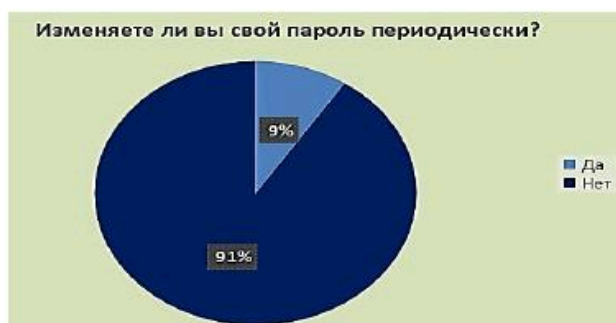


Рис. 6. Периодические изменения пароля

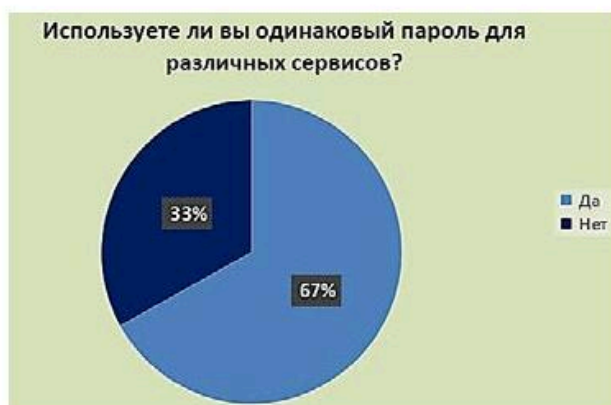


Рис. 7. Использование одинаковых паролей для различных сервисов

Литература

- [1] Шаньгин В.Ф. *Информационная безопасность компьютерных систем и сетей*. Москва, ИД «ФОРУМ», 2024, 416 с.
- [2] *Информационная безопасность. Противоречия психологии паролей*. URL: <https://www.infosecurity-magazine.com/news/the-contradictions-of-password-psychology/> (дата обращения 01.11.2024).
- [3] Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP. *Вопросы кибербезопасности*, 2015, № 2 (10), с. 60–68.
- [4] Nelson D., Vu K.-P.L. Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior*, 2010, iss. 4, pp. 705–715. <https://doi.org/10.1016/j.chb.2010.01.007>
- [5] Абидарова А.А. Анализ надежности паролей для обеспечения информационной безопасности. *Известия ТулГУ. Технические науки*, 2021, № 8, с. 66–68.

Psychological aspects of online security: choosing passwords

Gevorgyan E.A. gevorgyaneaa1@student.bmstu.ru

Potapov A.V. potapov@bmstu.ru

BMSTU (KB), Kaluga, Russia

The article considers the psychological aspects of choosing passwords for accounts. The reluctance to come up with a complex password and the problem of remembering it leads to the fact that it becomes easier for attackers to crack passwords and get confidential information. The purpose of the work is to report on the danger of choosing simple passwords due to the associative choice of words or symbols. The methods of choosing secure passwords and its security are described. A social experiment was conducted, statistics on the use of simple passwords were provided and a conclusion was made about people's awareness of password insecurity

Keywords: password, social engineering, psychology of choice, threat, danger, insecurity, account, hacking, security, confidentiality