ВОПРОСЫ АКТУАЛЬНОСТИ БЕЗОПАСНОСТИ ПАРОЛЕЙ

САХНО Виталий Викторович
магистрант
ПРОКАЗОВА Жанна Витальевна
магистрант
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

В настоящее время вопрос о безопасности паролей растет с каждым годом и становится все более актуальным. В результате преступлений злоумышленника страдают коммерческие предприятия. Сотрудники и клиенты несут материальные и моральные убытки, такие как кража денежных средств и распространение персональной информации.
Ключевые слова: информационная безопасность, пароль, целостность, конфиденциальность, доступность.

Наиболее часто объектами преступников становятся не только обычные пользователи, которые плохо знакомы с основами информационной безопасности, но и технически подготовленные. На данный момент угрозы кибербезопасности находятся не только во внимании аудиторских сообществ, но и в приоритете правительства. Пароль представляет собой некое секретное слово, предназначенное для подтверждения личности или полномочий.

Можно сказать, что информационная безопасность – это такое состояние защищенности информационных ресурсов, при котором обеспечены: доступность, целостность и конфиденциальность [1].

Для того чтобы определить важность безопасности паролей, разберем каждое свойство более подробно:

– конфиденциальность представляет собой свойство информации, которое гарантирует предоставление доступа к информации лишь тем пользователям, которые имеют доступ к ней;

– доступность – это свойство информации, которое предполагает, что лица, имеющие доступ к информации, могут в любой момент времени получить доступ к ней;

– целостность – это свойство информации, гарантирующее, что только определенные лица могут модифицировать или удалять информацию.

Пароль позволяет увеличить уровень безопасности хранения конфиденциальности, разграничить доступ к разной информации пользователям. Безопасность паролей – один из основных способов обеспечения высокой защиты информации, которая постоянно подвергается нападкам злоумышленников. Безопасность пароля зависит от стойкости его самого, способа и места его хранения, и конечно, от здравомыслия человека, работающего с ним.

Стойкость пароля – это некое количество времени, потраченное на подбор пароля каким-либо методом [2]. То есть, сколько времени потребуется злоумышленнику на подборку вашего пароля.

Существует несколько способов хранения паролей:

– в электронном виде (в приложениях и сервисах и т. д.);

– на бумаге (блокнот, тетрадь, напоминалка).

Для анализа используемых паролей обратимся к исследованию Троя Ханта, который взял за предмет своего исследования базу пользователей Sony Pictures [3].

Анализ приносит неутешительные выводы. Количество паролей с длиной от 6 до 10 символов показывает отличный результат, но у половины он менее 8 символов, что уменьшает стойкость пароля (рисунок 1). Высокая стойкость пароля определяется возможным чередованием букв различных регистров, цифр, спецсимволов (рисунок 2). К сожалению, люди

наиболее часто используют символы одного типа, что значительно снижает стойкость паролей. Использование уникальных символов позволяет в разы увеличить стойкость паролей, но результат неутешительный, 30% – это словарные слова (рисунок 3).

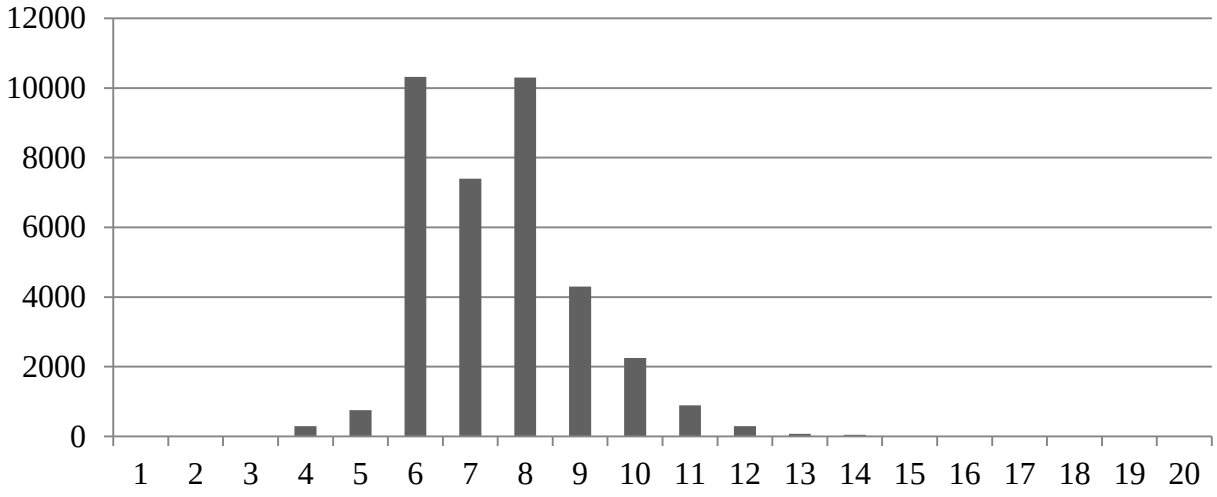

Рисунок 1. **Длина пароля**

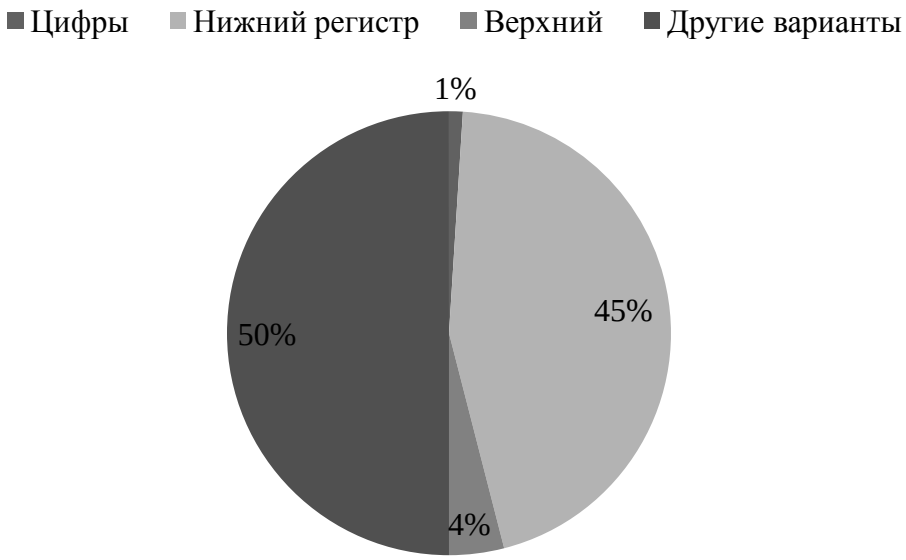

Рисунок 2. **Используемые символы**

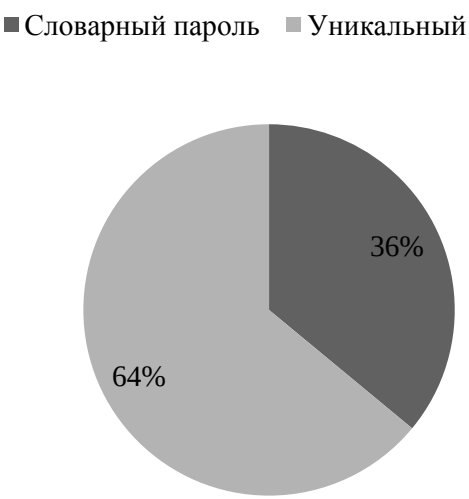

Рисунок 3. **Словарные пароли**

Можно выделить следующие способы получение пароля злоумышленником:

1. Перехват. Пароли могут быть украдены при передаче по интернету или сети.

2. Поиск. Информационные технологии позволяют искать сохраненные пароли в вашем устройстве (компьютер, телефон и т. д.).

3. Перебор. Автоматический перебор с помощью специальных программ.

4. Подглядывание. Даже такой простой метод зачастую позволяет узнать пароль.

5. Социальная инженерия. Мошенники применяют методы социальной инженерии для раскрытия паролей самими жертвами.

6. Key Logging. Установка специальных программ для похищения паролей в процессе их ввода (клавиатурный шпион).

Для наглядного примера проанализируем несколько паролей с помощью JavaScript анализатора, который был разработан в рамках проекта «Rumkin.com» [4]. Основная оценка пароля строится на использовании его энтропии, вычисление которой происходит на основе диаграмм для английского языка [5].

На основе данных о паролях можно вывести ряд рекомендаций, к которым должны прислушиваться пользователи при выборе пароля:

1. Длина пароля:

– для обычных пользователей - не менее 8 символов;

– для администраторов - не менее 15 символов.

2. Период смены пароля:

– административные – каждые 60 дней;

– пользовательские – каждые 90 дней.

3. Пароли должны содержать следующие символы (строчные буквы, прописные буквы, цифры, спецсимвол).

4. Пароли не должны составляться на каком-либо одном смысловом слове.

5. Пароли не должны основываться на типовых шаблонах (asdfg, 987654321, ytrewq).

СПИСОК ЛИТЕРАТУРЫ

1. *Витенбург Е.А., Левцова А.А.* Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов // Вестник Донского государственного технического университета. – 2018. – № 18(3):333-338. – URL:https://doi.org/10.23947/1992-5980-2018-18-3-333-338.

2. Кибербезопасность – О надежности пароля и об использовании хеш-функции. – URL: https://newtechaudit.ru/kiberbezopasnost-o-nadezhnosti-parolya/ (дата обращения: 17.08.2021).

3. Исследование на тему паролей. – URL: https://habr.com/ru/post/129052/ (дата обращения: 17.08.2021).

4. Еще об оценки стойкости пароля. – URL: https://habr.com/ru/sandbox/27520/ (дата обра-

щения: 17.08.2021).
5. Strength Test. – URL: https://www.rumkin.com/tools/password/passchk.php (дата обращения: 17.08.2021).

PASSWORD SECURITY RELEVANCE ISSUES

SAKHNO Vitaly Viktorovich
undergraduate
PROKAZOVA Zhanna Vitalievna
master student
Don State Technical University
Rostov-on-Don, Russia

Nowadays, the issue of password security is growing every year and becomes more and more relevant. Business enterprises suffer as a result of the attacker's crimes. Employees and customers suffer material and moral losses, such as theft of funds and the dissemination of personal information.
Key words: information security, password, integrity, confidentiality, availability.