УДК 004.77

МЕТОДЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ПАРОЛЕЙ

Е.А. ЛАПТЕВА[1], А.К. СУБАЕВА[2]
[1] магистрант кафедры «Приборостроение»
[2] д.э.н., доцент кафедры «Приборостроение»
«Казанский национальный исследовательский технический университет им. А.Н. Туполева -КАИ»
Чистопольский филиал «Восток»,
г. Чистополь, Российская Федерация

Аннотация: В статье рассматривается проблема парольных систем идентификации и аутентификации пользователей. Основная задача исследования – изучить определения основных терминов, основные методы обеспечения уникальности паролей, а также провести анализ суммарной статистики используемых символов в паролях и выяснить, какие из комбинаций менее надежные. Изучена существующая литература по выбранной тематике.

Ключевые слова: идентификация, аутентификация, пароль, статистика, уникальность, анализ, пользователь.

PASSWORD-BASED USER IDENTIFICATION AND AUTHENTICATION METHODS

E.A. LAPTEVA, A.K. SUBAEVA
[1] master student of the Department of Instrument Engineering
[2] Doctor of Economics, Associate Professor
of the Department of Instrument Engineering
Kazan National Research Technical University named after A.N. Tupolev -KAI, Chistopol branch «Vostok»,
Chistopol, Russian Federation

Annotation: The article deals with the problem of password identification and user authentication systems. The main task of the study is to study the definitions of the main terms, the main methods of ensuring the uniqueness of passwords, as well as to analyze the total statistics of the

characters used in passwords and find out which combinations are less reliable. The existing literature on the chosen topic has been studied.

Key words: identification, authentication, password, statistics, uniqueness, analysis, user.

В современной эпохе отрасль информационных технологий стремительно прогрессирует, обнаруживая новые уязвимости и разрабатывая новые методы доступа к данным для нелегитимных пользователей. В связи с этим требуется постоянное внимание со стороны пользователей и лиц, ответственных за защиту информации, чтобы следить за новыми вызовами и способами обеспечения безопасности [1].

Одними из важных компонентов обеспечения безопасности в информационных системах являются идентификация и аутентификация.

Идентификация – это процесс распознавания пользователя по предварительно установленному описанию, аутентификация – проверка прав доступа пользователя к информации или определенным действиям. Различают одностороннюю и двустороннюю аутентификацию, а также методы на основе знаний пользователя, владения материальными объектами или биометрических данных [2].

Обеспечение безопасности систем и данных важно через проверку подлинности пользователя и установление его личности. Эти процессы позволяют предотвращать несанкционированный доступ, защищать конфиденциальность информации и обеспечивать целостность данных. Применение идентификации и аутентификации широко распространено в сферах информационных технологий, финансов и электронной торговли для обеспечения безопасного доступа к системам и информации.

Представим разнообразные методы проверки подлинности. При использовании пароля, важно соблюдать два противоположных правила: пароль должен быть сложным для угадывания и легким для запоминания.

Сложность пароля определяется количеством символов (N) и минимальной длиной (k). Общее количество возможных паролей $C = N\text{k}$ [2]. Срок действия пароля, отличие от логического имени и уникальность паролей - основные положения политики учетных записей пользователей. Противодействие попыткам взлома включает:

ограничение попыток входа, скрытие логина последнего пользователя, учет всех попыток входа. Система реагирует на неудачные попытки входа, блокируя учетную запись или устанавливая временную задержку. Хранение пароля в базе данных обычно зашифровано. Организация защиты паролей идентификации: список паролей, генерация на основе хеширования для устранения недостатков. Подтверждение подлинности при парольной аутентификации основывается на вводе конфиденциальной информации, которую можно подобрать или украсть.

Существует два метода для обеспечения уникальности паролей. Во-первых, можно установить определенный срок действия пароля, что заставит пользователя периодически менять его. Во-вторых, возможно вести реестр использованных ранее паролей для данного пользователя, который контролируется администратором. Однако исключить возможность выбора простых паролей пользователем, придерживаясь установленных правил, практически невозможно. Пользователь может использовать легкие пароли, не нарушая установленных ограничений. Для обеспечения надежности и уникальности паролей администратор КС может сам устанавливать пароли пользователям, запрещая им их изменение. Для генерации сложных паролей может применяться специальное программное обеспечение. Тем не менее, назначение паролей администратором может создать проблемы с передачей пароля, проверкой сохранения пароля пользователем и возможностью злоупотребления администратором своими правами. Поэтому наиболее разумным подходом является возможность пользователя выбирать пароль в соответствии с правилами администратора, с возможностью сброса пароля администратором при его утере [3].

Несмотря на то, что в идеале для сохранения своей личной информации необходимо придумывать уникальный пароль и периодически его менять, далеко не все люди хотят тратить на это свое время и используют легкие быстро-запоминающиеся пароли. Сводная информация о распространенных наборах символов, используемых в паролях российских пользователей приведена в таблице 1.

Таблица 1 – Сводная информация

Набор символов	Доля, %
Только цифры	57,73%
Символы английского алфавита в нижнем регистре	17,96%
Символы английского алфавита в нижнем регистре и цифры	17,51%
Символы английского алфавита в разных регистрах и цифры	3,4%
Символы английского алфавита в разных регистрах	1,63%
Символы английского алфавита в верхнем регистре и цифры	1,35%
Символы русского алфавита в нижнем регистре	1,12%

Также на рисунке 1 представлена визуальная диаграмма, демонстрирующая сводную информацию о распределении использованных наборов символов.

После проведения анализа паролей, применяемых российскими пользователями, были получены следующие результаты: около 47% исследованных паролей состоят из буквенных комбинаций, около 53% из цифровых комбинаций, а большинство пользователей предпочитают использовать пароли, которые не превышают восьми символов. Такое положение дел повышает вероятность успешных атак методом перебора, особенно в случае, когда дополнительные защитные механизмы не применяются.

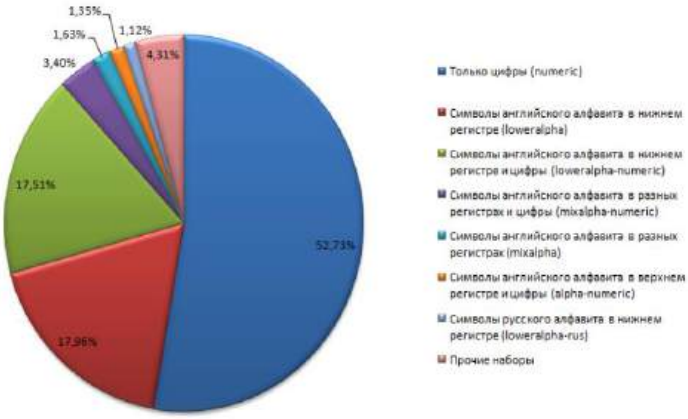

Рисунок 1 – Диаграмма сводной информации
о распределении символов

На втором месте по популярности находится использование только символов английского алфавита (маленьких букв), составляющих до 18% паролей. Затем идут пароли, включающие как символы английского алфавита (строчные символы), так и цифры. Эти комбинации составляют 17% от общего числа проанализированных паролей.

Таким образом, примерно 88% паролей, используемых российскими пользователями, включают в себя либо только цифры, либо строчные символы английского алфавита, либо же цифры и символы английского алфавита. Эти данные указывают на потенциальные уязвимости и необходимость улучшения практик создания и использования паролей с целью повышения безопасности информационных систем [4].

Дополнительным фактором, приводящим к созданию «слабого» пароля, являются стандартные критерии, приведенные в таблице 2.

Таблица 2 – Критерии «слабого» пароля в интернете

Причина «слабого» пароля	Доля, %
Полное совпадение пароля с именем пользователя	3,94%
Частичное совпадение пароля с именем пользователя	0,7%
Пароль содержится в публично распространяемых словарях	14,69%
Пароль является пустой строчкой	0,7%

На рисунке 2 представлено графическое отображение представленной таблицы.

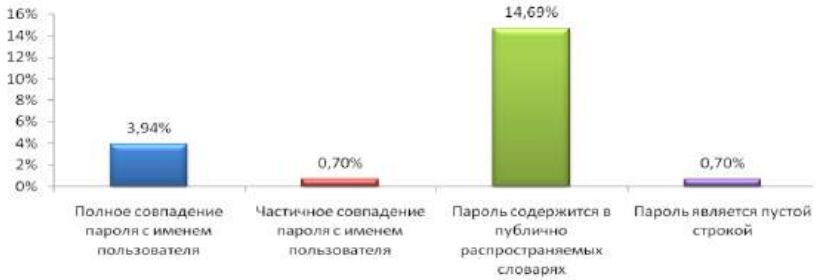

Рисунок 2 – Диаграмма критериев «слабого» пароля в интернете

Примерно 15% из проанализированных паролей содержаться в публично доступных словарях, а около 4% из них совпадают с использованными логинами, что в значительной степени упрощает людям с корыстными целями, работающими удаленно, получить несанкционированный доступ к имеющимся данным [4].

В современном мире защита данных и конфиденциальность информации играют ключевую роль. Эффективные системы аутентификации и пароли необходимы для обеспечения безопасности пользователей. Однако статистические данные свидетельствуют о том, что значительное количество пользователей выбирают слабые пароли, что представляет угрозу для их безопасности. Для повышения уровня защиты, рекомендуется использовать длинные и сложные пароли, включающие разнообразные символы, а также избегать предсказуемых комбинаций. В итоге, правильный подход к созданию

паролей является важным шагом к обеспечению безопасности персональных данных.

Также для обеспечения лучшей безопасности своего аккаунта и своих личных данных рекомендуется менять пароль раз в три месяца, или же еще чаще в зависимости от ценности данных, а также использовать методы двухэтапной идентификации.

ЛИТЕРАТУРА

1. Алгоритмы аутентификации пользователей. [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/16566572/page:30/ (дата обращения: 18.03.2024).

2. Идентификация и аутентификация. [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/articles/galatenko/ (дата обращения: 18.03.2024).

3. Парольные системы идентификации и аутентификации пользователей. [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/2648681/page:13/ (дата обращения: 18.03.2024).

4. Анализ проблем парольной защиты в Российских компаниях. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Metrics-Passwords-2009.pdf (дата обращения: 18.03.2024).

REFERENCES

1. Algoritmy autentifikacii pol'zovatelej. [Elektronnyj resurs]. – Rezhim dostupa: https://studfile.net/preview/16566572/page:30/ (data obrashcheniya: 18.03.2024).

2. Identifikaciya i autentifikaciya. [Elektronnyj resurs]. – Rezhim dostupa: http://citforum.ru/security/articles/galatenko/ (da-ta obrashcheniya: 18.03.2024).

3. Parol'nye sistemy identifikacii i autentifikacii pol'zovatelej. [Elektronnyj resurs]. – Rezhim dostupa: https://studfile.net/preview/2648681/page:13/ (data obrashcheniya: 18.03.2024).

4. Analiz problem parol'noj zashchity v Rossijskih kompa-niyah. [Elektronnyj resurs]. – Rezhim dostupa:

https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-Metrics-Passwords-2009.pdf (data obrashcheniya: 18.03.2024).