УДК: 004.35

ПАРОЛИ: ИХ ОСОБЕННОСТИ И ВАРИАНТЫ

Грачева Е.И., студент гр. 21401, IV курс
Научный руководитель: Субаева А. К, д.э.н., доцент
Чистопольский филиал «Восток» Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ
г. Чистополь

В эпоху цифровизации и повсеместного проникновения интернет-сервисов вопросы защиты конфиденциальных данных выходят на первый план.

Конфиденциальность данных – это необходимость защиты от утечки информации, которая ограничена по доступу и представляет ценность для правообладателя [1].

Несмотря на развитие биометрических и аппаратных методов аутентификации, парольная защита остается наиболее распространенным, а зачастую и единственным барьером между злоумышленником и учетной записью пользователя. Главная проблема заключается в противоречии: надежные пароли сложны для запоминания, а простые — легко подбираются.

Систематизируем знания об особенностях создания паролей и анализе современных вариантов управления ими для обеспечения баланса между безопасностью и удобством использования.

Пароль - это набор специальных символов для ввода в определённой строке, когда требуется подтверждение вашей личности на этапе аутентификации, в момент получения доступа к определённому ресурсу [1].

Рассмотрим особенности создания и использования паролей, на которые может повлиять человеческий фактор. Выявлена прямая корреляция между удобством запоминания и низкой стойкостью пароля. Установлено, что повторное использование одного и того же пароля на разных сервисах является критической уязвимостью (эффект "домино"). Определено, что включение в пароль цифр, спецсимволов и букв разного регистра экспоненциально увеличивает время его подбора методом грубой силы [1].

Рассмотрим варианты защиты паролем с технологической точки зрения. Следует использовать многоразовые текстовые пароли – это классический вариант. Рекомендуемая длина — не менее 12-14 символов. Основной недостаток — необходимость запоминания. Так же в современном мире пользователи активно используют одноразовые пароли (OTP) как второй фактор защиты [1]. Пароли генерируются приложением (Google Authenticator) или приходят по SMS. Эффективны против перехвата данных при повторном вводе. Очень популярны и фразы-пароли. Это вариант создания длинной последовательности

из случайных слов ("правильный-батарейка-скрепка-конь"). Такие пароли легко запоминаются, но очень сложны для подбора. Так же существуют графические пароли. Они используются в мобильных устройствах (рисунок на сетке точек). Удобны для сенсорного ввода, но уязвимы для "грязных" экранов**.** Самый надежный и эффективный метод – это менеджеры паролей [1].

Менеджер паролей – это программа, помогающая пользователям создавать надежные пароли, хранить их в цифровом хранилище, защищенном единым мастер-паролем, а затем по мере необходимости получать их при входе в учетные записи [1].

Большинство современных компаний используют проверенные криптографические технологии, которые представлены в таблице 1.

Таблица 1 – криптографические технологии

Технология	Область использования
AES-256(для шифрования данных)	Стандарт, который используют военные и спецслужбы
PBKDF2, Argon2 или scrypt(для создания ключей)	Функции делают подбор мастер-пароля вычислительно невозможным даже при наличии мощного оборудования
Zero-knowledge архитектура	Разработчики сервиса не имеют доступа к вашим расшифрованным данным
Двухфакторная аутентификация (2FA)	Дополнительный уровень защиты через приложения-аутентификаторы, SMS или аппаратные ключи.

Интеграция таких ПО в повседневную практику пользователя позволяет автоматически генерировать 20-значные пароли со всеми типами символов, что делает атаки перебором практически бесполезными. Оценочные расчеты показывают, что время подбора такого пароля даже на суперкомпьютерах превышает разумные временные рамки (сотни и тысячи лет) [2].

Оптимальным вариантом для современных пользователей является комбинация менеджера паролей и двухфакторной аутентификации. Так как менеджер паролей служит для генерации и хранения сложных комбинаций, а двухфакторная аутентификация для защиты наиболее важных аккаунтов.

Ключевыми особенностями надежного пароля являются – достаточная длина пароля (от 12 символов), отсутствие привязки к личным данным пользователя, использование различных групп символов и уникальность пароля для каждого сервиса.

Рассмотрим методы шифрования паролей. Самые популярные из них – это шифр Цезаря, шифр Виженера, шифр Атбаш, шифр Плейфера. Особенности данных шифров приведены в таблице 2.

Таблица 2 – Шифры и их особенности

Шифр	Особенности
Шифр Цезаря	Однородный сдвиг, простой ключ, уязвимость к частотному анализу, ограниченное количество ключей, алгоритмическая простота [3].
Шифр Виженера	Для шифрования используется ключевое слово, которое повторяется по длине исходного текста, каждая буква исходного текста сдвигается на величину, определяемую соответствующей буквой ключа, дешифрование происходит в обратном порядке [4].
Шифр Атбаш	Не требует вычислений, только знание алфавита; можно легко выполнить обратную операцию для дешифрования текста, если известен алфавит; шифр применяется только к одному алфавиту, не поддерживает числовые символы или другие языки [5].
Шифр Плейфера	Использует матрицу 5×5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4×8); содержит ключевое слово или фразу; в исходном шифре буквы «I» и «J» обычно считаются одним и тем же символом, чтобы поместиться в матрицу из 25 ячеек.

Рассмотрим примеры шифров Цезаря, Виженера, Атбаш на рисунках 1, 2, 3 соответсвенно:

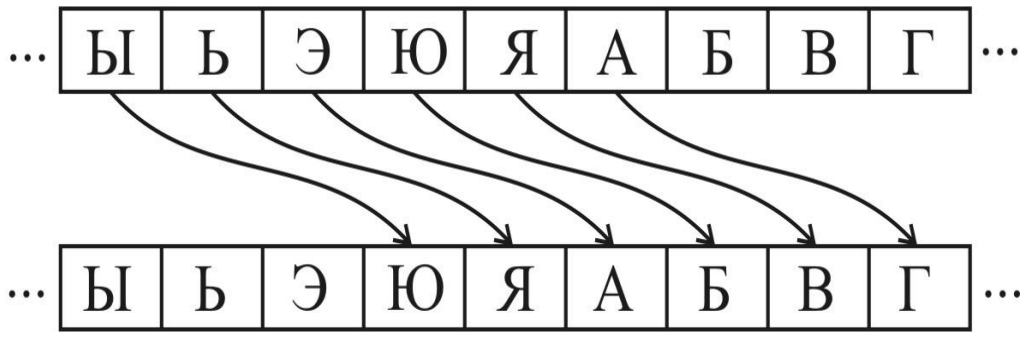

Рисунок 1 – Пример шифра Цезаря

P	R	O	G	R	A	M	- исходное сообщение
15	17	14	6	17	0	12	
D	O	G	D	O	G	D	- ключ
3	14	6	3	14	6	3	
18	5	20	9	5	6	15	- сумма по модулю
S	**F**	**U**	**J**	**F**	**G**	**P**	- криптограмма

Рисунок 2 – Пример шифра Виженера

б	в	г	д	ж	з	к	л	м	н
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
щ	ш	ч	ц	х	ф	т	с	р	п

Рисунок 3 – Пример шифра Атбаш

Шифры позволяют защитить личные данные, главное уметь ими пользоваться.

Отметим, что повышение и поддержание уровня безопасности напрямую зависит от информированности пользователей и использования современных инструментов аутентификации.

Таким образом, в данной статье были рассмотрены особенности создания и использования паролей, варианты защиты паролем, методы шифрования, а также ключевые особенности надежного пароля. Использование всех методов защиты позволит сделать ваш пароль надежнее и труднодоступнее для злоумышленников.

Список литературы:

1. Как защитить данные [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/protecting-your-data-online-password-manager (Дата обращения 16.03.2026)

2. Менеджер паролей [Электронный ресурс]. URL: https://www.securitylab.ru/blog/personal/Technolady/357119.php (Дата обращения 16.03.2026)

3. Шифр Цезаря [Электронный ресурс]. URL: https://repetitor.1c.ru/informatics/shifr-tsezarya/ (Дата обращения 16.03.2026)

4. Шифр Вижнера [Электронный ресурс]. URL: https://spravochnick.ru/informatika/vzlom_shifra_vizhenera/ (Дата обращения 16.03.2026)

5. Шифр Атбаш [Электронный ресурс]. URL: https://cipher-sonline.com/ru/shifr-atbash (Дата обращения 16.03.2026)