Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2021, № 1, с. 13-21.

Поступила: 15.01.2021
Окончательный вариант: 11.05.2021

© УлГУ

УДК 004.457

Разработка усовершенствованных генераторов паролей

Глотов А. И.*, Котилевец И. Д., Иванова И. А.

*shackkale@gmail.com
РТУ МИРЭА, Москва , Россия

В данной работе представлен анализ методов защиты пользовательских учётных записей. Был проведён опрос приоритетов пользователей при создании паролей и исследованы основные тенденции по защите аккаунтов. Описаны плюсы и минусы различных способов авторизации в системе. На основании полученных выводов был предложен новый метод генерации паролей с использованием парольных фраз и выдвинуты функциональные требования к разрабатываемому приложению с кратким описанием принципа его работы.

***Ключевые слова**: пароль, безопасность, пользовательские данные, аутентификация, учётная запись, аккаунт.*

Введение

Вопросы безопасности пользовательских данных в последнее время становятся всё более и более актуальными. В большинстве случаев аккаунты пользователей защищены весьма слабыми паролями, которые, ко всему прочему, могут повторяться на различных сервисных приложениях. Более того, пароли создаваемые пользователем из случайно сгенерированных последовательностей букв и чисел могут быть недостаточно надёжными при малой длине генерируемой последовательности, не говоря о том, что они также могут быть крайне сложными для запоминания. Для обеспечения безопасности учётных записей необходимо в первую очередь создавать достаточно сложные, но при этом легко запоминаемые пароли. В данной статье рассмотрены варианты решения проблемы создания эффективной парольной защиты.

1. Существующие подходы по генерированию паролей

По данным аналитиков, большинство утечек пользовательских аккаунтов связано с атаками на слабо защищённые учётные записи. Около 83% потерь аккаунтов происходят из-за слабой парольной защиты [1]. Для решения данной проблемы интернет-сервисы и организации используют различные методы, включая использование дополнительных факторов защиты (например, двухфакторная аутентификация, использование парольных хранилищ) и биометрию [2]. Однако в этих решениях есть свои минусы. Дополнительные факторы защиты не являются обязательными на большинстве сервисах и в основном служат в качестве вспомогательных мер обеспечения безопасности. Количество аккаунтов, использующих такие факторы, по данным из статистики Google, составляет около 10% от всех зарегистрированных пользователей [3]. Говоря о двухфакторной аутентификации, при потере одного из факторов защиты восстановление доступа в учётную запись становится затруднительным. А в случае специальных хранилищ для получения списка паролей необходимо использовать мастер-пароль, который, в свою очередь, может быть уязвимым. Биометрия имеет следующий ряд недостатков - во-первых, при повреждении фактора, по которому производится вход в систему (например, при повреждении подушечки пальца), пользователь временно теряет доступ к своей учётной записи до момента восстановления данного фактора защиты (т.е. до регенерации подушечки пальца). Кроме того, при утечке биометрических показателей смена ключа, по которому производится вход в аккаунт, становится достаточно трудной задачей, а в некоторых случаях - невозможной, если, например, в системе производится вход при помощи алгоритмов распознавания лица.

Использование паролей до сих пор остаётся самым эффективным способом защиты учётных данных. Существуют разные готовые программные решения по созданию сложных паролей. Они разделяются на два типа - пароли, представленные в виде случайной последовательности букв, чисел и символов, и парольные фразы из произвольных слов. Первый вид сложен для запоминания, использовать такие пароли без менеджера паролей представляется крайне затруднительным. Второй вариант является наиболее практичным с точки зрения как безопасности, так и удобства использования в случае, если пользователь не желает использовать парольные хранилища [4]. Примерная оценка взлома пароля грубым перебором при относительно одинаковой сложности [5] представлена на рисунке ниже (рис. 1):

Password	TIme to crack
`p%9y#k&yFm?`	Approximately 90,182,663 centuries
`logic finite eager ratio`	Approximately 189,658,722 centuries

Рис. 1. Сравнение сложности разных подходов к генерированию паролей.

Однако эти пароли являются уязвимыми для атаки перебора по словарю в случае, если комбинация слов слишком мала или же является предсказуемой [6].

В качестве сравнения разрабатываемого решения с уже существующими продуктами можно взять менеджер паролей RoboForm. Данная программа позволяет пользователю генерировать пароли с сильной защитой и сохранять их у себя в менеджере. Так же за дополнительную плату данное решение позволяет синхронизировать сохранённые пароли на всех устройствах, на которых оно установлено. К тому же существует возможность держать все используемые для входа данные либо на облачном хранилище, либо на локальной диске.

Однако данное решение имеет недостаток большинства парольных менеджеров. Для защиты учётной записи в данном ПО в любом случае нужно будет создать достаточно сложный, устойчивый и легко запоминаемый мастер-пароль, который будет использоваться пользователем для дальнейшего входа в хранилище.

2. Эффективность использования сгенерированных парольных фраз.

Парольные фразы легче использовать чем случайные сгенерированные последовательности символов в основном из-за особенностей свойств памяти и процессов запоминания информации у человека. Семантическая память хранит словесные знания, благодаря ней, люди способны понимать смысл отдельных элементов предложения, воспроизводить ассоциации с определёнными образами каждого слова. Человеку крайне сложно оперировать статистическим данными, которые не вызывают никакой подсознательной реакции. Национальный Институт Стандартов и Технологий (NIST) в своих рекомендациях объяснял это так - нам куда проще вспомнить букву, следующую за «s», нежели чем 20 символ в английском алфавите [7]. Это основная причина, по которым людям удобнее запоминать парольные фразы вместо случайного набора символов, не имеющих никакого смыслового значения.

Для решения проблемы уязвимости к атакам перебора по словарю можно использовать случайные сгенерированные словосочетания [8]. Когда пользователь самостоятельно попытается придумать парольную фразу, состоящую из нескольких слов, в его предложении будут появляться закономерности, которые могут сократить общее количество возможных вариантов паролей [9]. Используя случайную выборку, можно таким образом решить проблему с этими закономерностями. Вдобавок ко всему, замена определённых букв на символы и добавление случайно спецсимволов в парольную фразу значительно повысит общее количество возможных вариантов ключей и, тем самым, усложнит задачу подбора пароля.

3. Результаты опроса пользователей

В качестве решения вышеописанных проблем была выдвинута идея разработки улучшенных генераторов парольных фраз. Для разработки такого генератора была собрана

статистика из анкеты предпочтений пользователей при создании паролей и учтены данные, проанализированные на WP Engine [9]. По проведённому опросу можно отметить следующие факторы:

- большинство пользователей используют слова в своих паролях (рис. 2);
- анкетируемые чаще используют более абстрактные словосочетания, не связанные с их данными (рис. 3);
- подавляющее большинство отдают предпочтение коротким паролям, предположительно используя небольшие словосочетания для входа в учётные записи (рис. 4):
- больше половины опрашиваемых используют в своих паролях спецсимволы (рис. 5), и добавляют их либо в начале пароля, либо в конце (рис. 6).
- пароли, в которых происходят слишком частые замены символов и в которых используется большое количество букв разных регистров, являются трудными для запоминания (рис. 7):
- пользователи почти не используют местоимения в паролях (рис. 8):

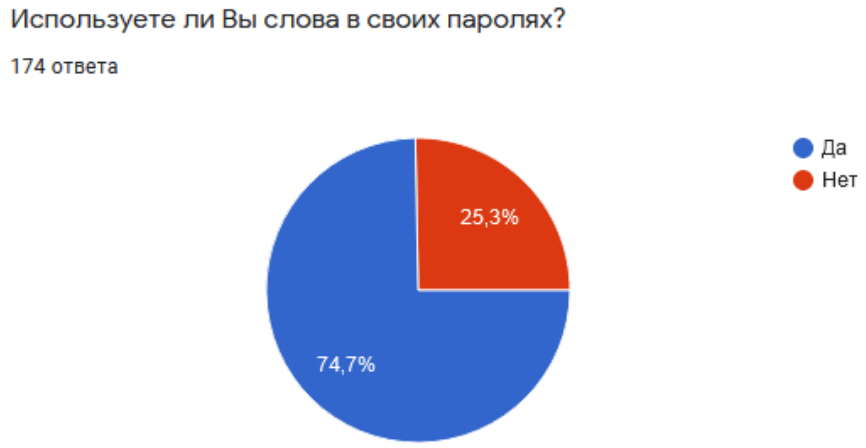

Рис. 2. Процент использования слов в паролях.

Рис. 3. Процент пользователей, использующих в своих паролях абстрактные слова.

Рис. 4. Статистика по наиболее удобной длины пароля.

Рис. 5. Статистика использования спецсимволов в паролях.

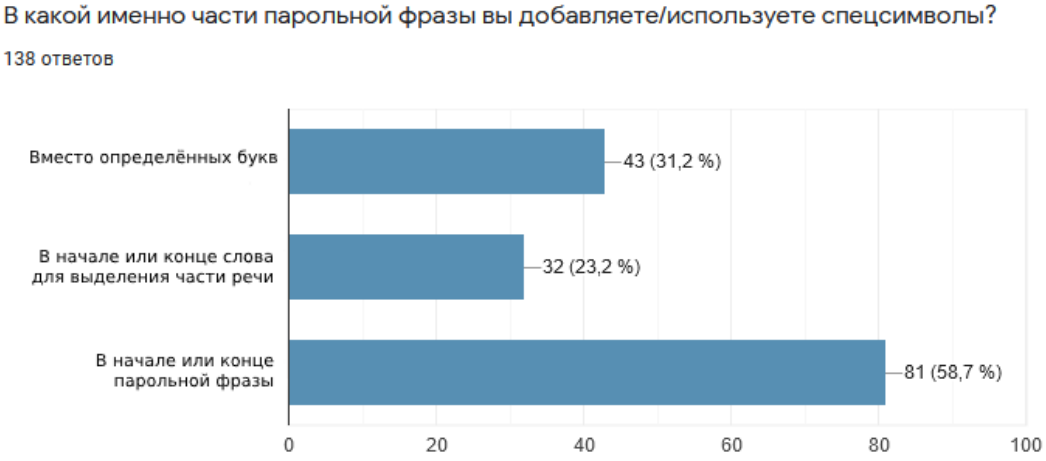

Рис. 6. Статистика по использованию спец символов в паролях.

Рис. 7. Оценка сложности пароля.

Рис. 8. Оценка использования местоимений.

4. Разработка решения

Учитывая статистику, а также недостатки прочих решений по созданию паролей, можно предположить следующее решение: использовать генераторы парольных фраз состоящих из случайных словосочетаний, заменяя некоторые буквы в самих словах на похожие символы и цифры, добавляя также возможность пользователю выделять определённые части речи при помощи тех же спецсимволов. Количество выбранных заменяемых букв в среднем будет составлять 1-3 буквы на всё парольное предложение. Рекомендованная длина пароля должна составлять около 20 символов [10], минимальная по стандарту NIST 800-63B - 8 символов [11]. Для удобства пользователя, генератор должен быть реализован в виде плагина для браузера. Таким образом, пароли будут генерироваться достаточной сложности, чтобы быть устойчивыми как к атакам полного посимвольного

перебора, так и к атакам перебора по словарю. При этом, сложность запоминания такого пароля повысится незначительно, а использования генератора в виде расширения для браузера сделает генератор наиболее удобным пользователю для использования. Диаграмма работы разрабатываемого приложения представлена на рис. 9.

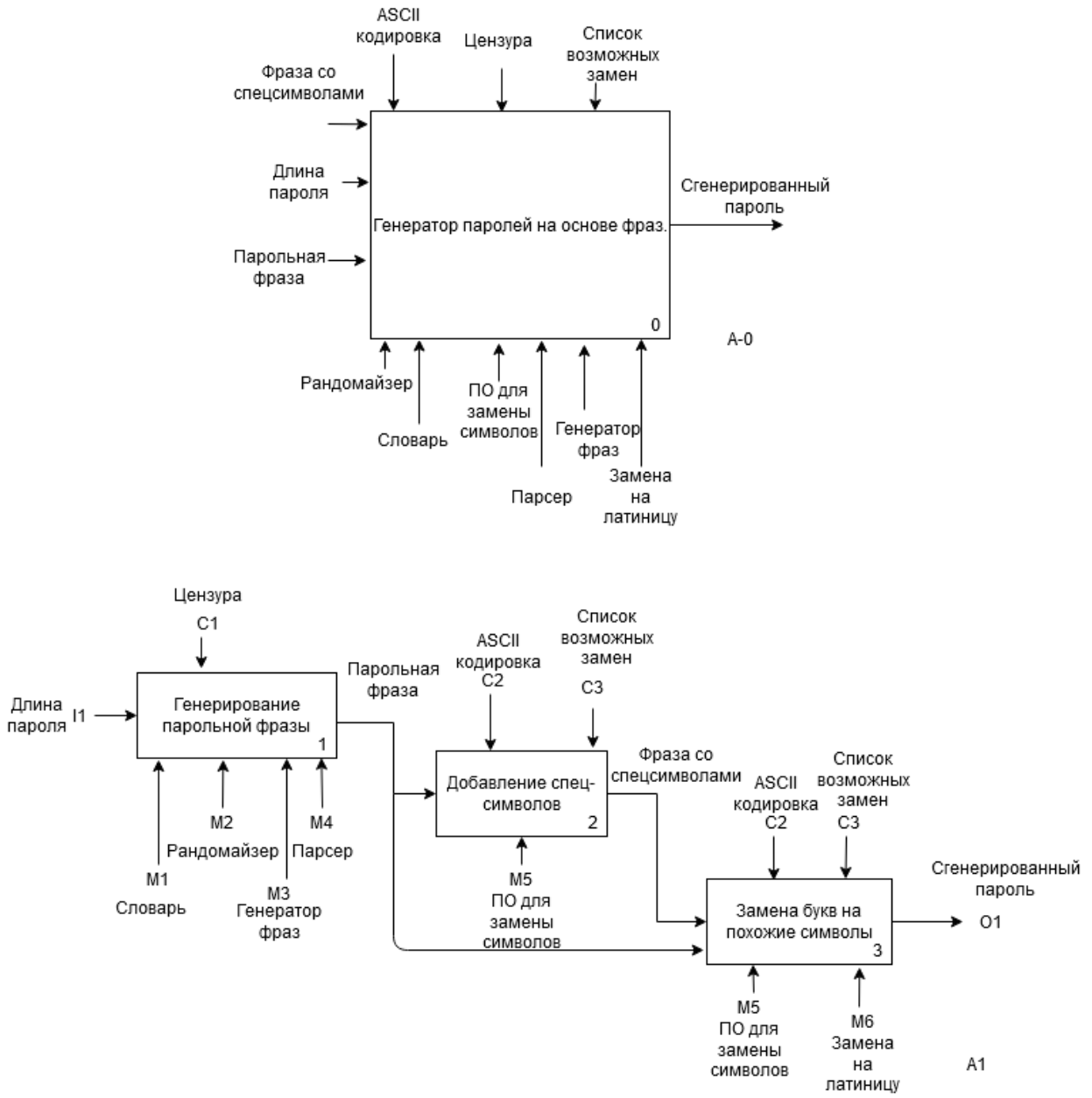

Рис. 9. IDEF0 диаграмма работы приложения.

Исходя из вышеперечисленных предложений, были выдвинуты следующие функциональные требования по разработке генератора паролей:

- в паролях произвольно должна заменяться одна или несколько букв на похожие цифры и спецсимволы;
- генератор должен предоставлять возможность опционально выделять определённые части речи в парольной фразе при помощи спецсимволов;

- парольные фразы могут быть разделены между собой наиболее удобным пользователю способом;
- минимальная длина генерируемого пароля должна составлять не менее 20 символов;
- программа должна быть оформлена в виде расширения для браузера;
- генератор не должен использовать дополнительные части речи, таких, как местоимения, союзы и т.д;
- расширение будет реализовано с использованием следующего инструментария: JavaScript (с API), XUL+HTML+CSS, webextension-polyfill (под разработку на браузер Mozilla Firefox).

Заключение

Подводя итог, вопросы безопасности пользовательских учётных записей несомненно являются крайне важными для любого приложения. По этой причине необходимо обеспечить должную защиту аккаунтов при помощи устойчивых паролей, при этом не нагружая пользователя задачей запоминания сложных последовательностей символов.

По результатам данного исследования была предложена разработка усовершенствованного варианта генератора парольных фраз. Главными особенностями данного генератора являются удобство использования для обычного пользователя, возможность кастомизации, устойчивость к атакам перебора, лёгкость запоминания в случае, если пользователь отказывается использовать менеджеры паролей.

Список литературы

1. IANS. 83% online users think up their own, weak passwords. Режим доступа: https://www.gadgetsnow.com/tech-news/83-online-users-think-up-their-own-weak-passwords/articleshow/75912094.cms (дата обращения: 20.11.2020).
2. Suzanne C. What’s the solution to the growing problem of passwords? You, says Microsoft. Режим доступа: https://news.microsoft.com/features/whats-solution-growing-problem-passwords-says-microsoft/ (дата обращения: 20.11.2020).
3. Сычёв И. Google: почти никто не пользуется двухфакторной аутентификацией. Режим доступа: https://habr.com/en/news/t/409577/ (дата обращения: 20.11.2020).
4. Энтони Т. Почему парольные фразы удобнее паролей. Режим доступа: https://turumburum.ua/blog/pochemu-kodovye-slova-udobnee-paroley/ (дата обращения: 20.11.2020).
5. Use a Passphrase. Режим доступа: https://www.useapassphrase.com/ (дата обращения: 20.11.2020).
6. Гуфан Ю. К, Новосядлый В. А, Эдель Д. А. Оценка стойкости парольных фраз к методам подбора. Режим доступа: https://cyberleninka.ru/article/n/otsenka-stoykosti-parolnyh-fraz-k-metodam-podbora (дата обращения: 04.02.2021).

7. M. Garcia. Easy Ways to Build a Better P@$5w0rd. Режим доступа: https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd (дата обращения: 21.02.2021)
8. Тюрин К. А, Сёмин Р. В. Анализ стойкости парольных фраз на основе информационной энтропии. Режим доступа: https://cyberleninka.ru/article/n/analiz-stoykosti-parolnyh-fraz-na-osnove-informatsionnoy-entropii (дата обращения: 15.02.2021)
9. WP Engine. Unmasked: What 10 million passwords reveal about the people who choose them. Режим доступа: https://wpengine.com/resources/passwords-unmasked-infographic/ (дата обращения: 21.02.2021)
10. Tamás S. Какова оптимальная длина пароля (Перевод). Режим доступа: https://habr.com/ru/company/domclick/blog/515064/ (дата обращения: 20.11.2020).
11. NIST Special Publication 800-63B. Digital Identity Guidelines. Authentication and Lifecycle Management. Режим доступа: https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 21.02.2021)