**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

**ДОКЛАД**

на тему Системы управления паролями

*дисциплина: Математические основы защиты информации и информационной безопасности*

Студент: Каримов Зуфар Исматович

Группа: НФИмд-01-22

**МОСКВА**

2022г.

**Содержание**

[**Введение** 3](#_Toc118168508)

[**Что такое управления паролями?** 4](#_Toc118168509)

[**Распространенные ошибки** 4](#_Toc118168510)

[**Как сделать пароль более надежным?** 5](#_Toc118168510)

[**Как защитить пароль** 6](#_Toc118168510)

[**Заключение** 7](#_Toc118168511)

[**Список литературы** 8](#_Toc118168512)

**Введение**

Всё больше и больше личной информации в нашей жизни находятся в защищённых паролями аккаунтах — медицинские сведения, банковские счета и многое другое. Аккаунты сегодня защищены паролями. Если кто-то сможет узнать ваш пароль, он может получить доступ к вашему аккаунту и делать с ним все то, что можете и вы. И поскольку мы живём в сети, как мы можем защитить наши данные?

**Что такое управление паролями?**

Пароль – это набор или строка символов, которые дают нам доступ к компьютеру или учетной записи в Интернете. А управление — это набор принципов и рекомендаций, которые помогают пользователю создавать, изменять, организовывать и контролировать пароли, чтобы быть максимально безопасными.

Пароли — это ключи для доступа к вашему компьютеру, банковскому счету и практически ко всему, что вы делаете онлайн. Другими словами, пароли обеспечивают первую линию защиты от запрещенного доступа к вашим данным.

И одним из важных способов обеспечить себе безопасность своих данных в Интернете – это защитить пароли.

**Распространенные ошибки**

|  |  |  |
| --- | --- | --- |
| ошибка | пример | Оценка риска |
| Использование общего пароля | 12345678  qwertyui | Слишком рискованно, это первые догадки злоумышленников |
| Использование пароля, основанного на личных данных (псевдонимы, названия книг, группы) | гладиатор  hala madrid | Слишком рискованно, кто знает, легко может угадать эту информацию |
| Использование короткого пароля | John1234  Jimq1974 | Чем короче пароль, тем больше возможностей увидеть, угадать и взломать |
| Использование одного пароля везде | Использование одного пароля на каждом сайте | Рискованно. Если кто-то узнает об этом пароле, остальные учетные записи будут под угрозой |
| Записать свой пароль | Записать пароль на заметке или где-нибудь еще | Высокий риск, потому что любой, кто увидит заметку, может войти в вашу учетную запись |

**Как сделать пароль надежным?**

**Сила в разнообразии**

Секрет предотвращения угадывания, кражи или сброса пароля заключается в большом числе случайностей. Когда злоумышленники пытаются угадать пароли, они обычно делают две вещи: 1) используют «словари» — списки часто используемых паролей, и 2) делают случайные догадки. Чем длиннее и уникальнее ваш пароль, тем меньше вероятность его угадать одним из этих методов.

**Длина пароля = 3 символа**

**Первый символ = строчные буквы (26 вариантов) + прописные буквы (26 вариантов) = 52**

**Второй символ = 52 (такой же, как первый символ)**

**Третий символ = 52 (так же, как первый и второй символы)**

**Всего = 52 ^ 3 = 52 \* 52 \* 52 = 140608 комбинаций**

**Теперь давайте повторим процесс, но допустим, что нам разрешено добавлять цифры к паролю, но одинаковой длины (только 3 символа):**

**Длина пароля = 3 символа**

**Первый символ = строчные буквы (26 вариантов) + прописные буквы (26 вариантов) + цифры (10 вариантов) = 62**

**Второй символ = 62 (аналогично первому символу)**

**Третий символ = *62 (так же, как первый и второй символы)***

***Всего = 62 ^ 3 = 62 \* 62 \* 62 = 238328 комбинаций***

**Помощь от менеджера паролей**

Что такое менеджер паролей? Это ПО, которое помогает пользователю работать с паролями. То есть у подобной программы имеется база данных, которые содержат зашифрованные данные пароля. Многие менеджеры паролей работают как заполнитель формы. Другими словами, они заполняют данные пользователя автоматически в формах. Обычно они встроены в браузерах.

Но существует и обратная сторона медали. Мы не должны полностью полагаться на какой-то тип менеджера паролей потому что при использовании функции генератора паролей, менеджер паролей может использовать слабый генератор случайных чисел и пароли могут быть легко угаданы.

**Двухфакторная аутентификация (2FA)**

Двухфакторная аутентификация — отличный способ повысить уровень вашей безопасности. При создании нового аккаунта некоторые веб-сайты дадут вам возможность добавить «второй фактор» в процесс входа на него. Часто это подразумевает привязку вашего номера телефона к аккаунту, так что после ввода пароля вам будет предложено ввести код безопасности, присланный непосредственно вам. Таким образом, даже если у злоумышленника получится узнать ваш пароль, он всё равно не сможет попасть в аккаунт, поскольку у него не будет доступа к вашему телефону.

**Как защитить пароль?**

Нужно быть очень осторожным при использовании ваших паролей на общедоступных ПК, таких как школы, университеты, библиотеки и т.д. Не используйте функции сохранения пароля, такие как функция автозаполнения Google Chrome или функция автозаполнения Microsoft, особенно на общедоступных ПК. Не заполняйте какую-либо форму в Интернете своей личной информацией, если только вы не уверены, что можете ей доверять.

Следите за базой данных PwnedList, чтобы проверить, есть ли ваше имя пользователя или адрес электронной почты в списке утечек данных учетной записи в Интернете.

**Заключение**

В современном информационном веке пароли являются жизненно важным аспектом вашей безопасности. Они являются защитной линией фронта и наиболее широко используемым методом аутентификации, который обеспечивает защиту учетных записей пользователей вашего компьютера или сетевых учетных записей.  Чтобы быть по-настоящему надежным и безопасным, вам необходимо локально хранить зашифрованную копию базы данных паролей, по возможности использовать многофакторную аутентификацию, просматривать последние новости о безопасности, оценивать свои пароли и часто их менять.

**Список литературы**

* <https://gadgetshelp.com/bezopasnost/rukovodstvo-po-upravleniiu-paroliami/>
* <https://support.microsoft.com/ru-ru/windows/%D1%81%D0%BE%D0%B7%D0%B4%D0%B0%D0%BD%D0%B8%D0%B5-%D0%B8-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-%D0%BD%D0%B0%D0%B4%D0%B5%D0%B6%D0%BD%D1%8B%D1%85-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D0%B5%D0%B9-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>
* <https://support.mozilla.org/ru/kb/vybor-bezopasnogo-parolya-dlya-zashity-vashej-lich>