ИТМО

Факультет программной инженерии и компьютерной техники

Лабораторная работа №5

«Аудит паролей с помощью менеджера паролей»

по дисциплине «Информационная безопасность»

Выполнил:

Студент группы P3432

Чмурова М.В.

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2025

Задание

1. Установите бесплатный менеджер паролей (например, Bitwarden).
2. Создайте новую учетную запись и мастер-пароль высокой надежности.
3. Проанализируйте пароли, которые вы используете в своих аккаунтах (например, в соцсетях, почте). Оцените их слабость (проверьте, не были ли они скомпрометированы, через сервис https://haveibeenpwned.com/ - используйте только email, не пароль!).
4. Для 5 своих аккаунтов создайте с помощью менеджера новые надежные пароли (не менее 12 символов, буквы разного регистра, цифры, спец. символы) и сохраните их в менеджере.
5. Настройте генерацию одноразовых кодов (TOTP) для 2FA для одного из аккаунтов (если он поддерживается).

Выполнение

В первую очередь был установлен менеджер паролей Bitwarden. Во время регистрации был создан мастер-пароль высокой надежности из 12 символов, включая цифры, буквы разного регистра и специальные символы:

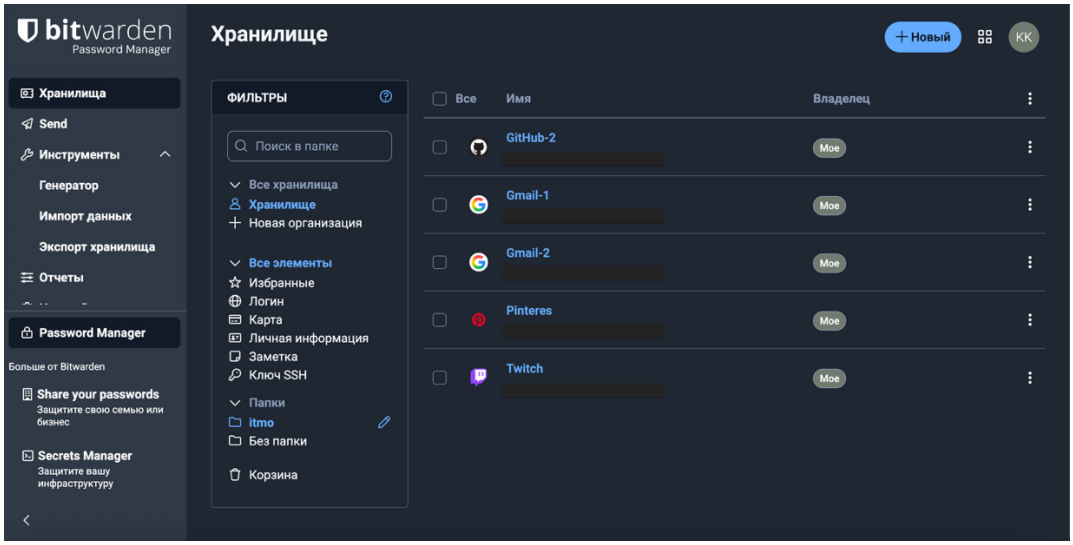

Рисунок 1. Настройка Bitwarden

Анализ паролей

Анализируя свою почту на утечки с помощью сайта https://haveibeenpwned.com/ - для одной из основных почт было найдено 4 утечки за период с 2018 по 2024 года:

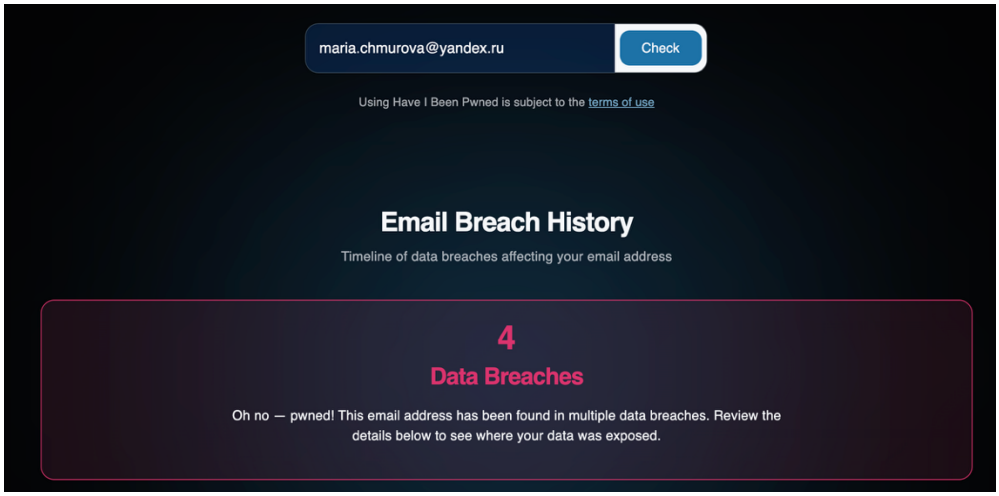

Рисунок 2. Найденные утечки

Две из них содержали хэши паролей bcrypt и MD5 с сайтов Wattpad и Shein.

Анализируя свои используемые пароли, могу сделать вывод, что в целом пароли, которые я использую – сильные, так как они используют

- буквы обоих регистров
- цифры
- специальные символы

Однако чаще всего это вариация одного и того же пароля с изменением некоторых символов. То есть эти пароли не идентичные, однако визуально очень похожи и зная один из них есть возможно наугад подобрать другой.

Кроме того, мои пароли являются старыми и некоторые из них могли оставаться однотипными >5 лет.

Одноразовые коды для 2FA

2FA – двухфакторная аутентификация – метод защиты доступа к данным, при котором необходимо подтверждение с двух разных факторов. То есть 2FA добавляет дополнительный уровень защиты.

Для настройки одноразовых кодов через Bitwarden для примера я воспользуюсь аккаунтом на GitHub. Для этого необходимо получить *setup key* – чтобы Bitwarden мог создавать коды для двухфакторной аутентификации:

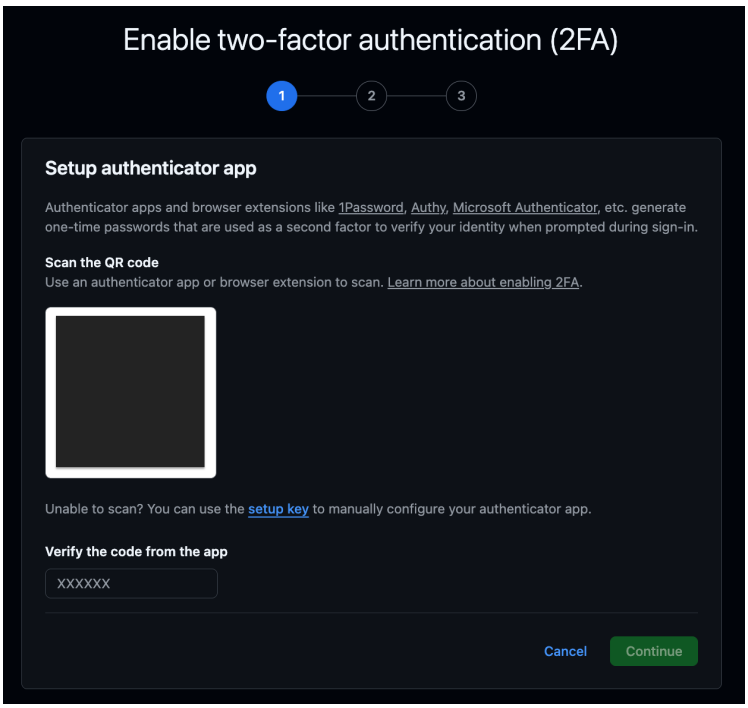

Рисунок 3. Настройка 2FA

После настройки в Bitwarden теперь имеется доступ к коду подтверждения (TOTP), который будет необходимо вводить при попытке входа в мой GitHub аккаунт:

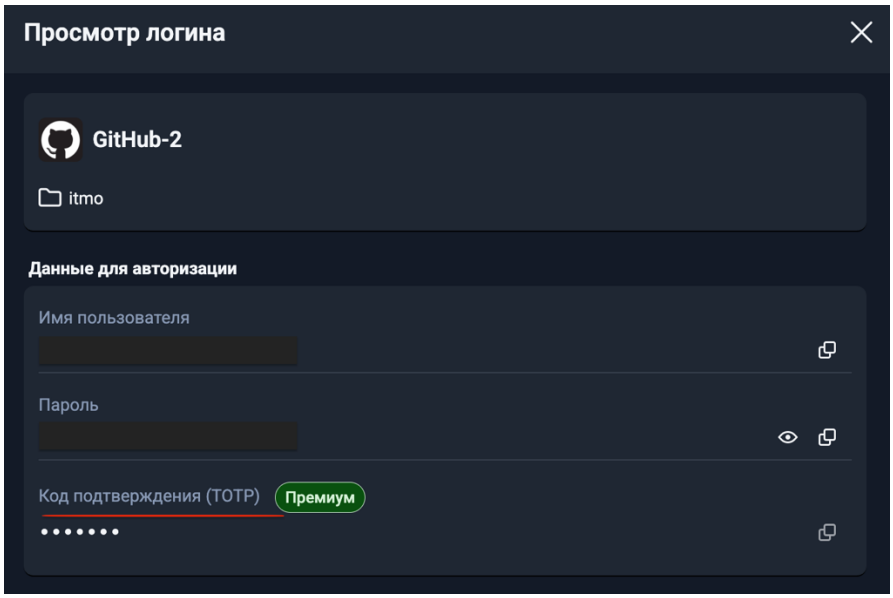

Рисунок 4. Настройка TOTP

Таким образом, 2FA теперь позволяет защитить мой аккаунт от взлома даже в случае утечки пароля или попадания его к злоумышленникам на фишинговых сайтах.

Вывод

В ходе данной лабораторной работы был проведен анализ надежности используемых мной паролей. Выяснилось, что они не идеальны, а также попадали под утечку на нескольких сайтах. С помощью использования Bitwarden я смогла настроить новые сильные пароли, а также настроить двухфакторную аутентификацию для одного из своих аккаунтов, что помогло усилить его защиту в разы.