Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа №5

«Аудит паролей с помощью менеджера паролей»

Барсуков Максим Андреевич

Группа: P3415

2025

Выполнение

Создание и настройка менеджера паролей

Создадим аккаунт на BitWarden: укажем свою почту, подтвердим ее, придумаем мастер-пароль, как показано на рисунке 1:

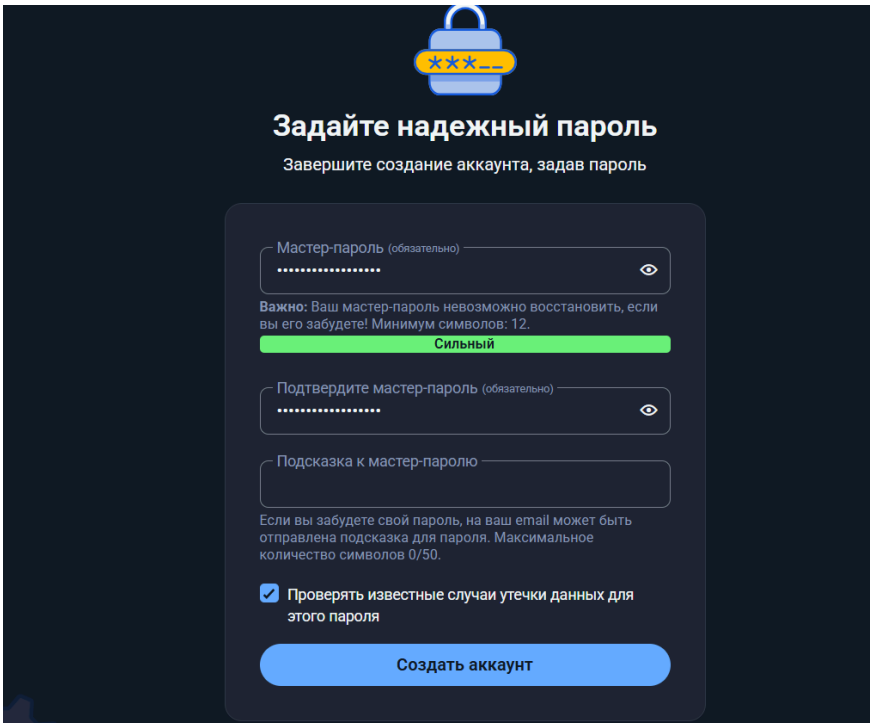

Рисунок 1 — Ввод мастер-пароля для создания учетной записи

После успешного создания учетной записи, можем увидеть хранилище BitWarden, как показано на рисунке 2:

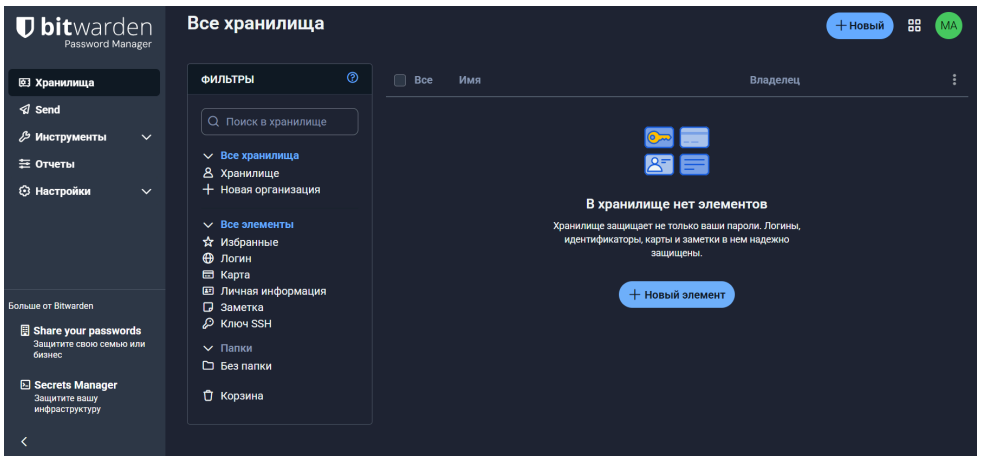

Рисунок 2 — Основное окно хранилища BitWarden

Проверим, не были ли они скомпрометированы мои пароли с помощью сервиса https://haveibeenpwned.com/. Как показано на рисунке 3, не обнаружено утечек, связанных с моей основной почтой:

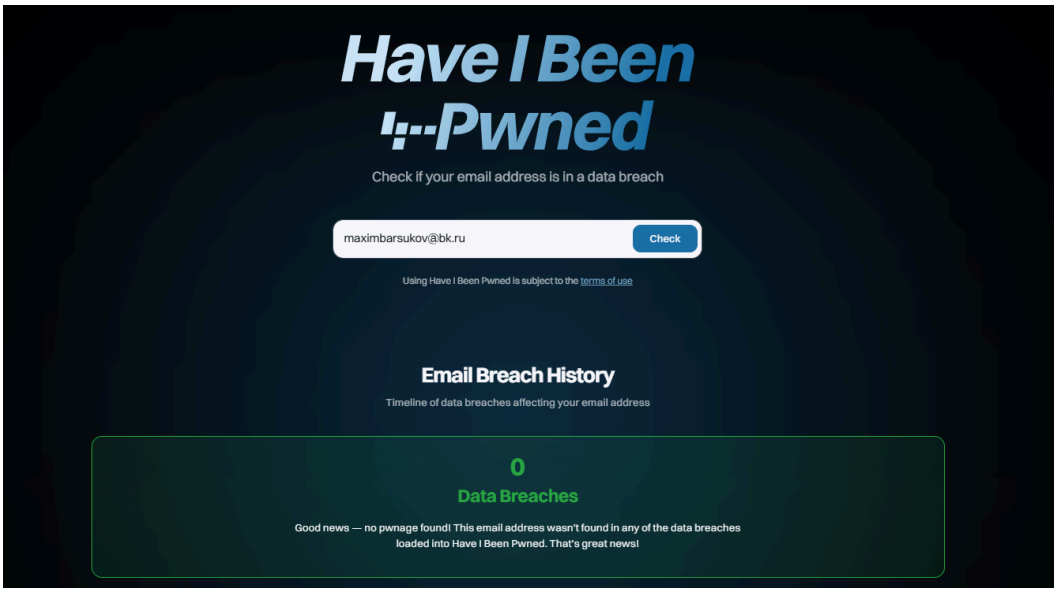

Рисунок 3 — Проверка на утечки для основной почты

Аудит и замена паролей для 5 аккаунтов

Так как скомпрометированных аккаунтов найдено не было, определим аккаунты, нуждающиеся в замене паролей другим способом.

Я обнаружил, что для 4 моих аккаунтов на разных площадках использовался **один и тот же пароль, состоящий из 8 символов одного регистра и без спец. символов**, поэтому менять пароли я буду для этих сайтов, а также для Steam (так как кража аккаунта грозит прямыми финансовыми потерями).

Итак, будем менять пароли для следующих платформ:

1. store.steampowered.com

Как показано на рисунках 4 и 5, пароль был изменен:

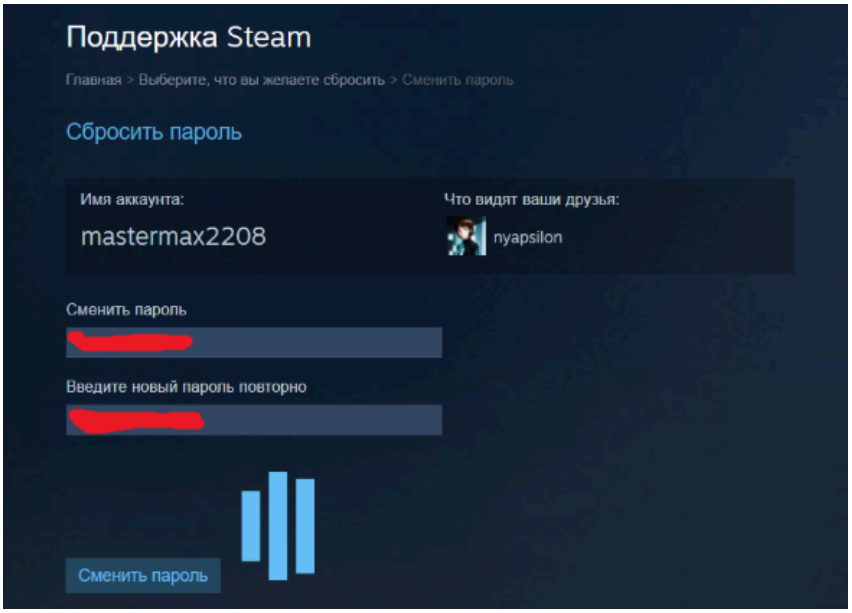

Рисунок 4 — Сброс пароля для Steam

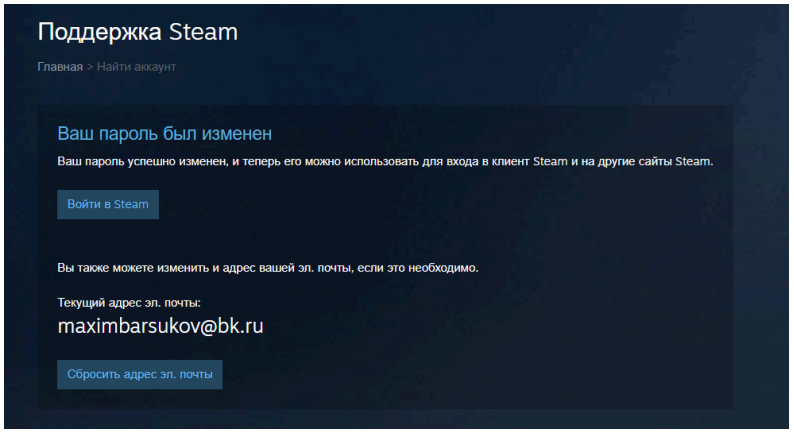

Рисунок 5 — Пароль Steam был изменен

2. bsky.app

   Как показано на рисунках 6 и 7, пароль был изменен:

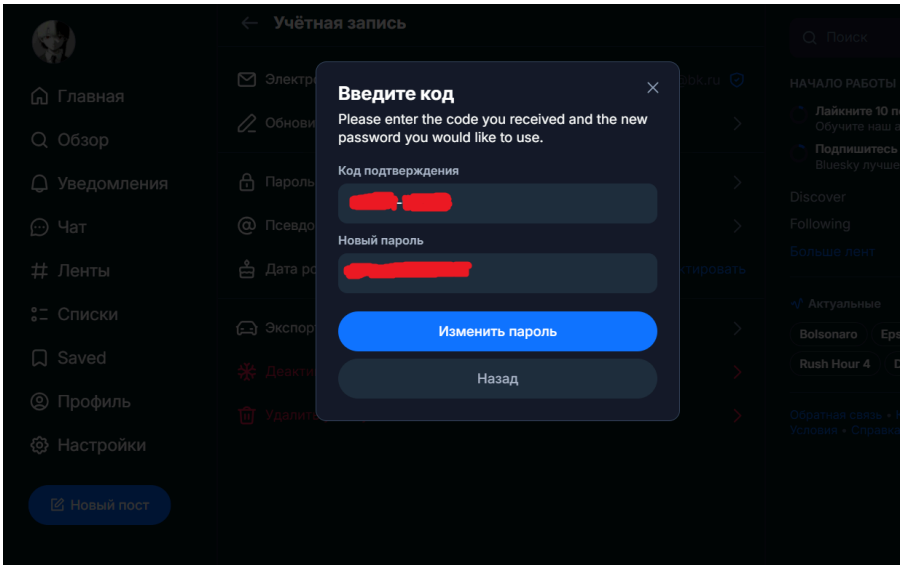

Рисунок 6 — Сброс пароля для Bluesky

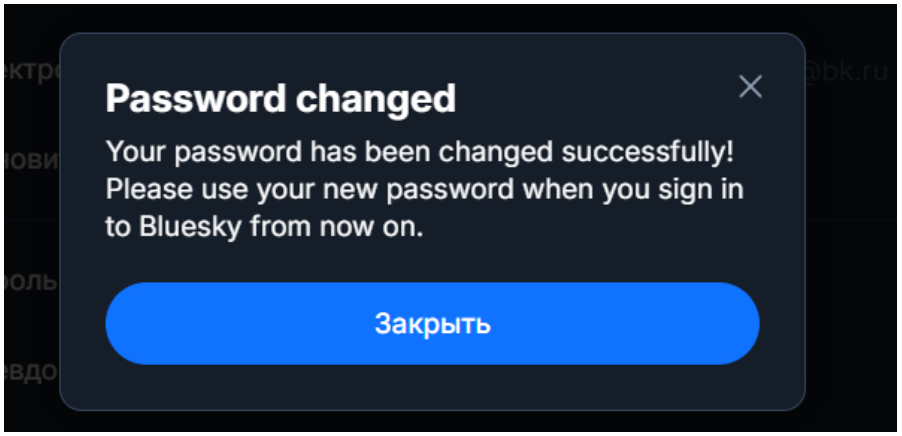

Рисунок 7 — Пароль Bluesky был изменен

3. hh.ru

Как показано на рисунках 8 и 9, пароль был изменен:

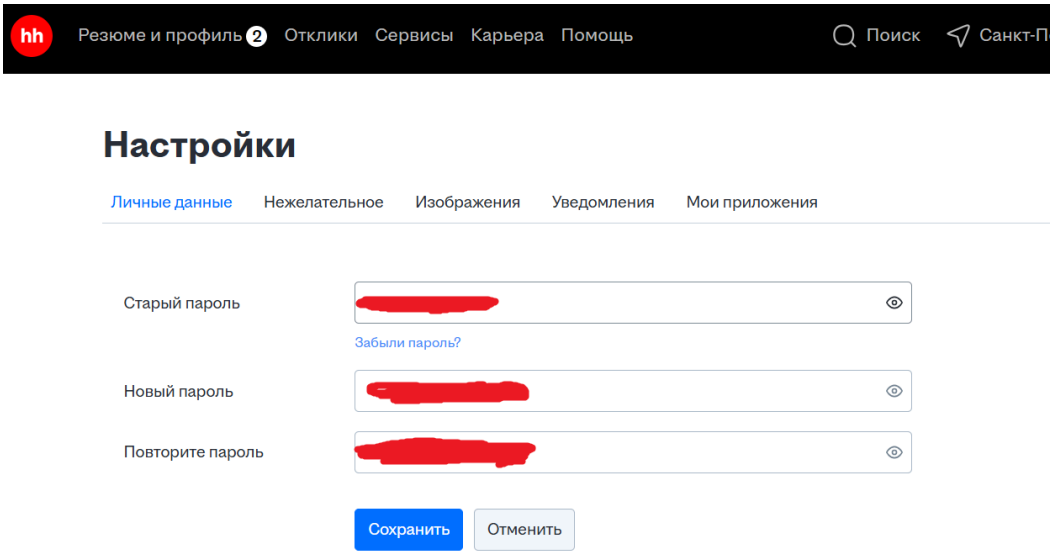

Рисунок 8 — Сброс пароля для HH

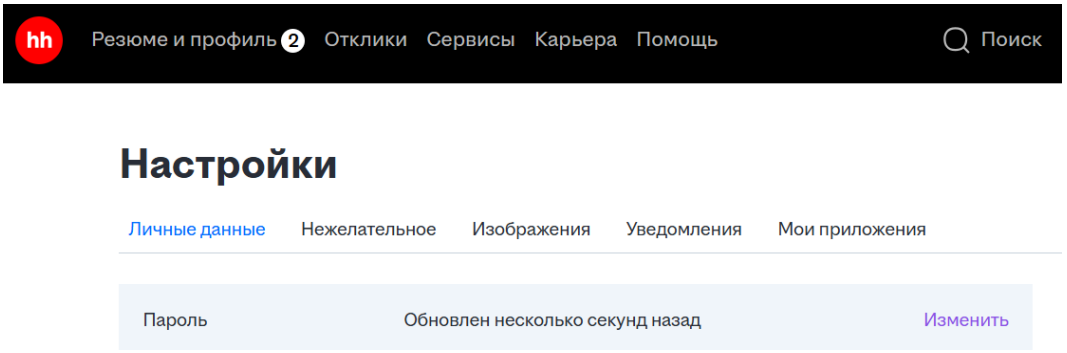

Рисунок 9 — Пароль HH был изменен

4. avito.ru

   Как показано на рисунке 10, пароль был изменен:

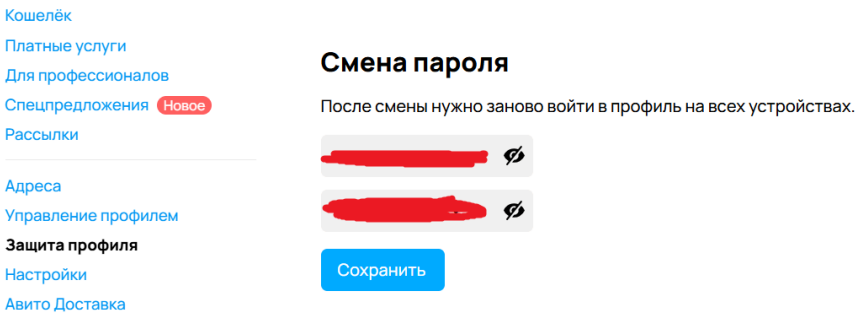

Рисунок 10 — Пароль Avito был изменен

5. habr.com

   Как показано на рисунках 11 и 12, пароль был изменен:

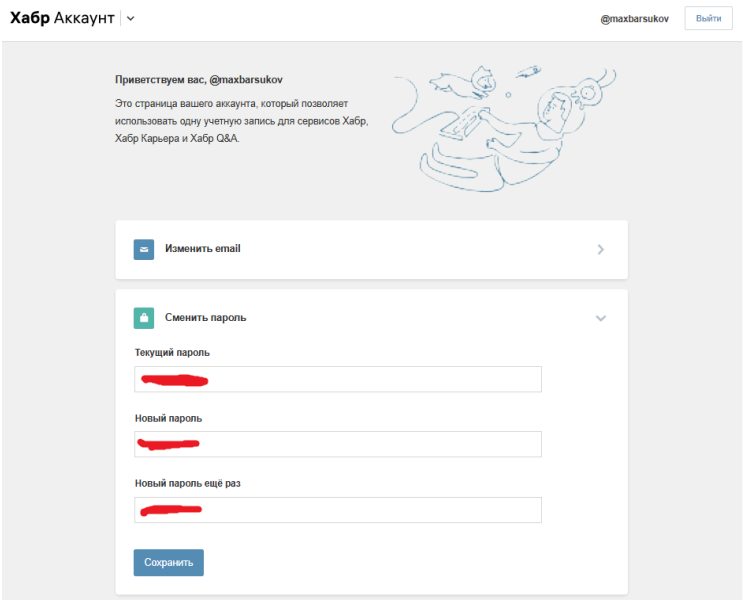

Рисунок 11 — Сброс пароля для Habr

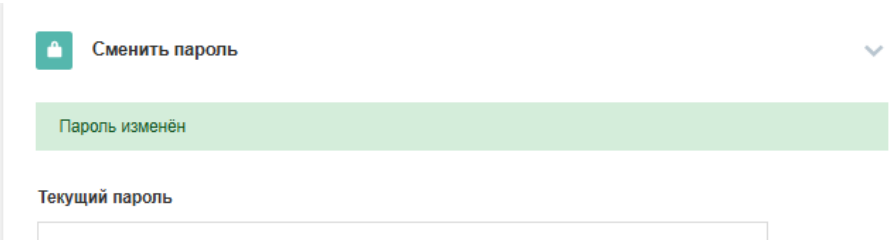

Рисунок 12 — Пароль Habr был изменен

После замены всех паролей на пяти аккаунтах, добавим аутентификационные данные в хранилище, как показано на рисунке 13:

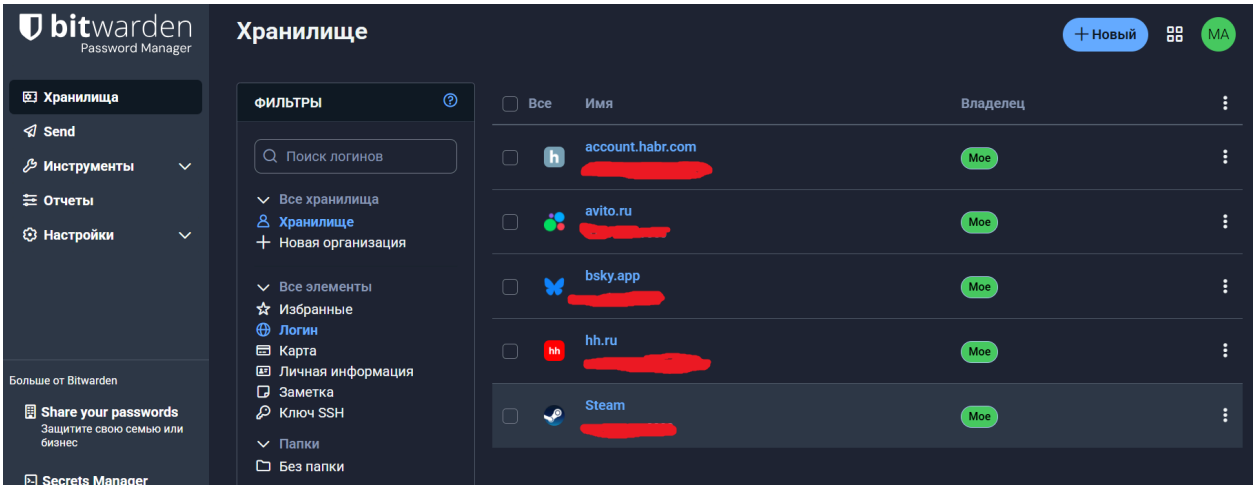

Рисунок 13 — Записи в BitWarden аккаунтов с новыми паролями

Анализ паролей (что было слабым)

Проведя аудит паролей, я в первую очередь отказался от их хранения в браузере. Анализ показал, что, хотя мои старые пароли формально соответствовали базовым требованиям безопасности (имели разный регистр, цифры и спецсимволы), их основная слабость заключалась не в длине, а в предсказуемости.

Несмотря на внешнюю сложность, они часто строились по одному и тому же шаблону. Например, я использовал схожие приёмы — добавление символов в начало и конец базового слова или замену букв на похожие цифры. Подобные пароли уязвимы для целевого перебора с использованием специальных правил и словарей.

В рамках этой работы я устранил этот ключевой недостаток, внедрив принцип децентрализации шаблонов. Новые пароли генерируются случайно, с использованием всего разнообразия символов на клавиатуре. Такой подход делает их устойчивыми не только к простому перебору, но и к сложным алгоритмам, которые анализируют возможные закономерности в структуре пароля.

Двухфакторная аутентификация

Двухфакторная аутентификация (или 2FA, Two-Factor authentication) – это метод защиты учетной записи, предполагающий предоставление сразу двух различных типов доказательств, чтобы убедиться, что пользователь – тот, за кого себя выдает.

Эти доказательства (факторы) бывают трех типов:

1. Что-то, что человек знает (знания) — пароль, пинкод.
2. Что-то, что у человека есть (владение) — одноразовый код из приложения-аутентификатора (тот же BitWarden или Google Auth), SMS на телефон, может даже физический ключ безопасности.
3. Что-то, чем человек является (биометрия) — отпечаток пальца или сканер лица применяются наиболее часто.

Двухфакторная аутентификация (2FA) служит дополнительным барьером безопасности, основанным на факторе владения. Это означает, что даже если злоумышленник получит пароль, этого будет недостаточно для доступа. Ему потребуется также физический доступ к вашему мобильному устройству или приложению, генерирующему одноразовые коды.

Хотя можно использовать универсальные менеджеры вроде Bitwarden или приложения-аутентификаторы (например, Google Authenticator), в данной работе мы рассмотрим встроенную систему самого сервиса. Платформа **Steam** предлагает собственную реализацию **2FA через мобильное приложение — Steam Guard**.

Для его активации необходимо привязать номер телефона к учетной записи. После этого вход в аккаунт будет возможен только после подтверждения через мобильное приложение Steam.

Приступим к настройке. Изначальное состояние показано на рисунке 14:

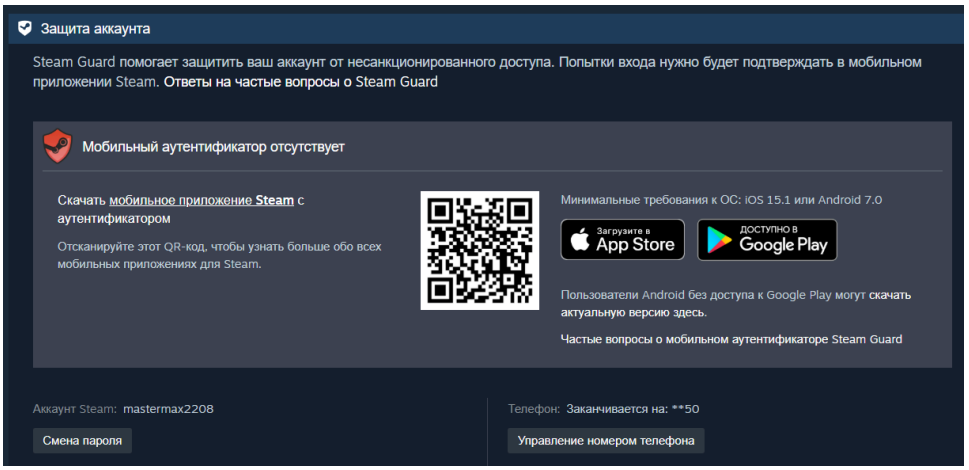

Рисунок 14 — До установки мобильного аутентификатора

Далее устанавливаемый мобильный аутентификатор, входим в аккаунт, после чего добавляем аутентификатор, как показано на рисунке 15:

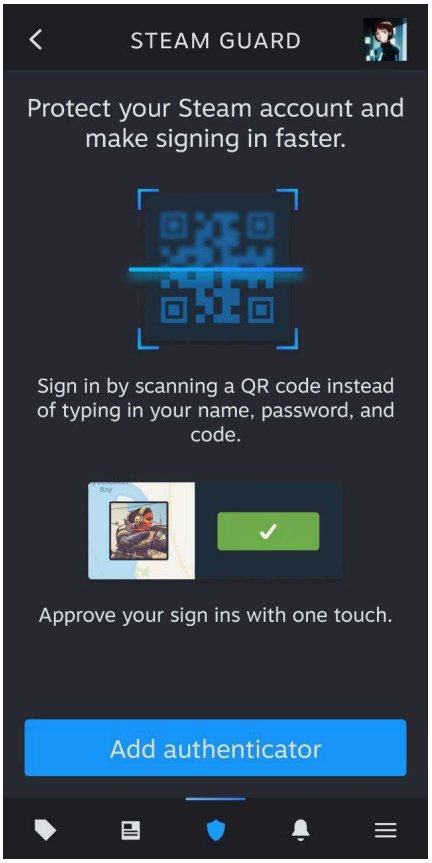

Рисунок 15 — Добавление мобильного аутентификатора

Дальше подтверждаем кодом из СМС, как показано на рисунке 16:

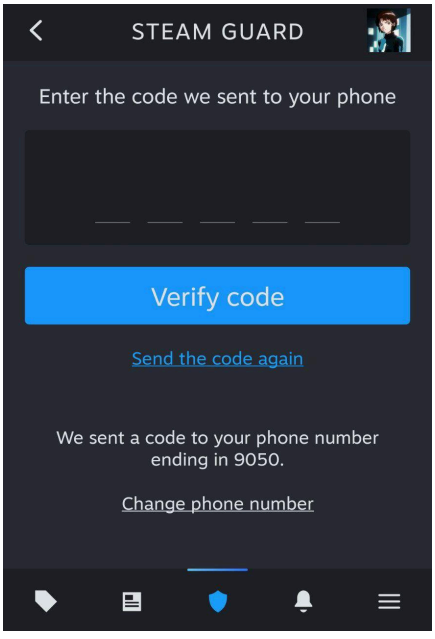

Рисунок 16 — Подтверждение кода из СМС

Дальше нам предлагают записать код для полного восстановления аккаунта в случае потери мобильного устройства, как показано на рисунке 17:

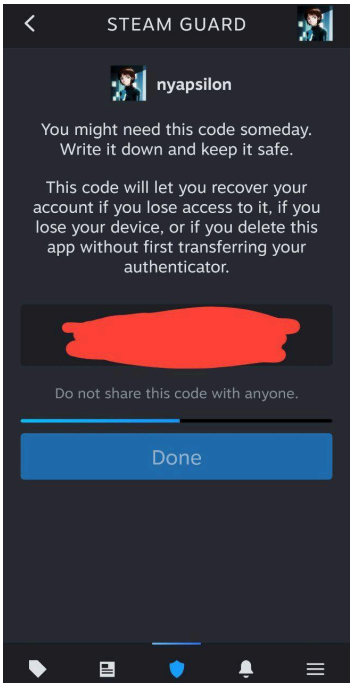

Рисунок 17 — Код восстановления

Теперь видим, что одноразовые коды начали приходить, как показано на рисунке 18:

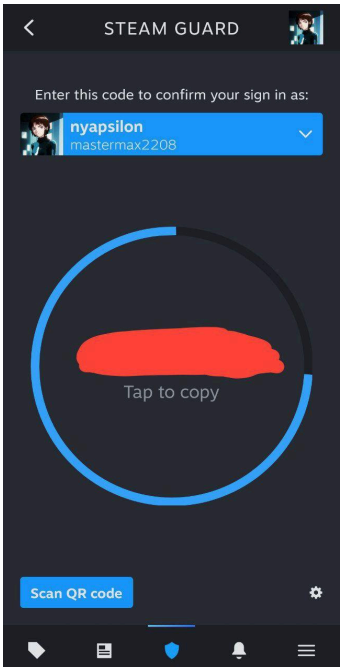

Рисунок 18 — Двухфакторная аутентификация Steam

Далее при каждом входе в аккаунт нужно либо ввести вот этот одноразовый код, либо навести камеру на QR-код с помощью приложения Steam, как показано на рисунке 19:

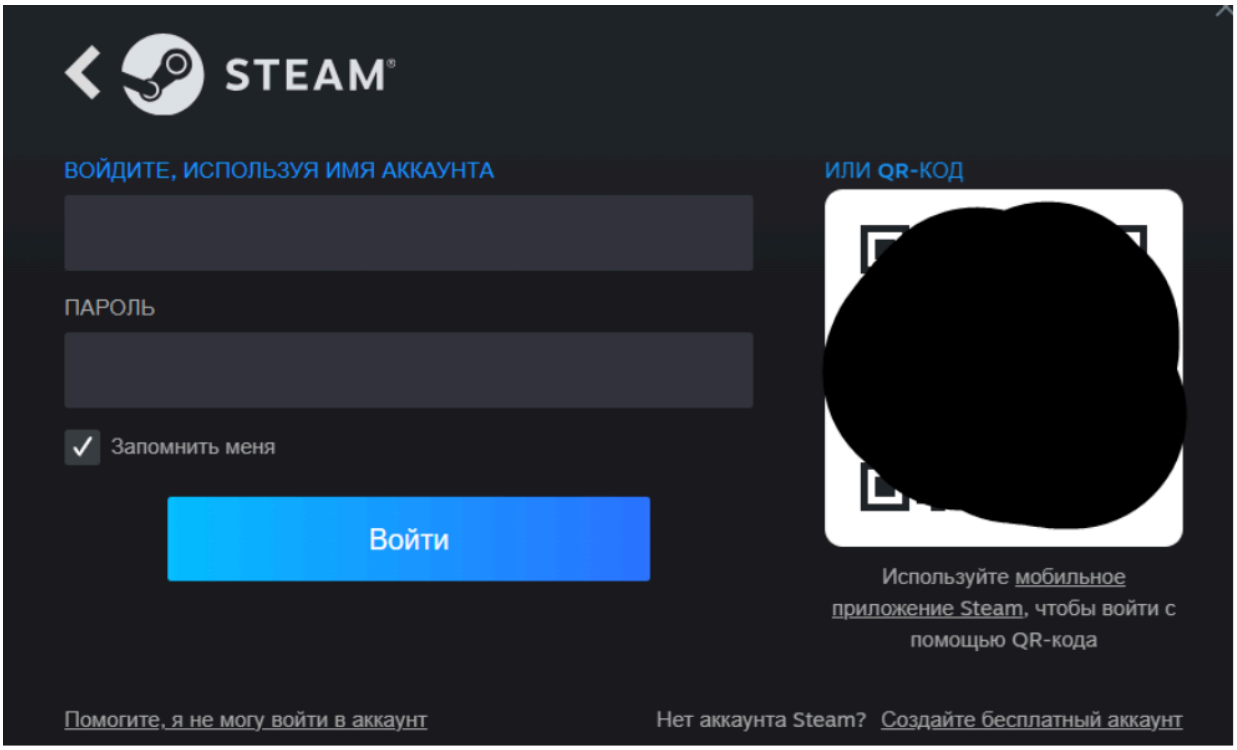

Рисунок 19 — QR-код для мобильного аутентификатора Steam