Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет ИТМО»
Факультет программной инженерии и компьютерной техники

Лабораторная работа №5

«Аудит паролей с помощью менеджера паролей»

Дисциплина «Информационная безопасность»

Выполнил:
Студент группы P3431
Нодири Хисравхон

Преподаватель:
Маркина Татьяна Анатольевна

г. Санкт-Петербург
2025г.

Содержание

1 Создание и настройка менеджера паролей

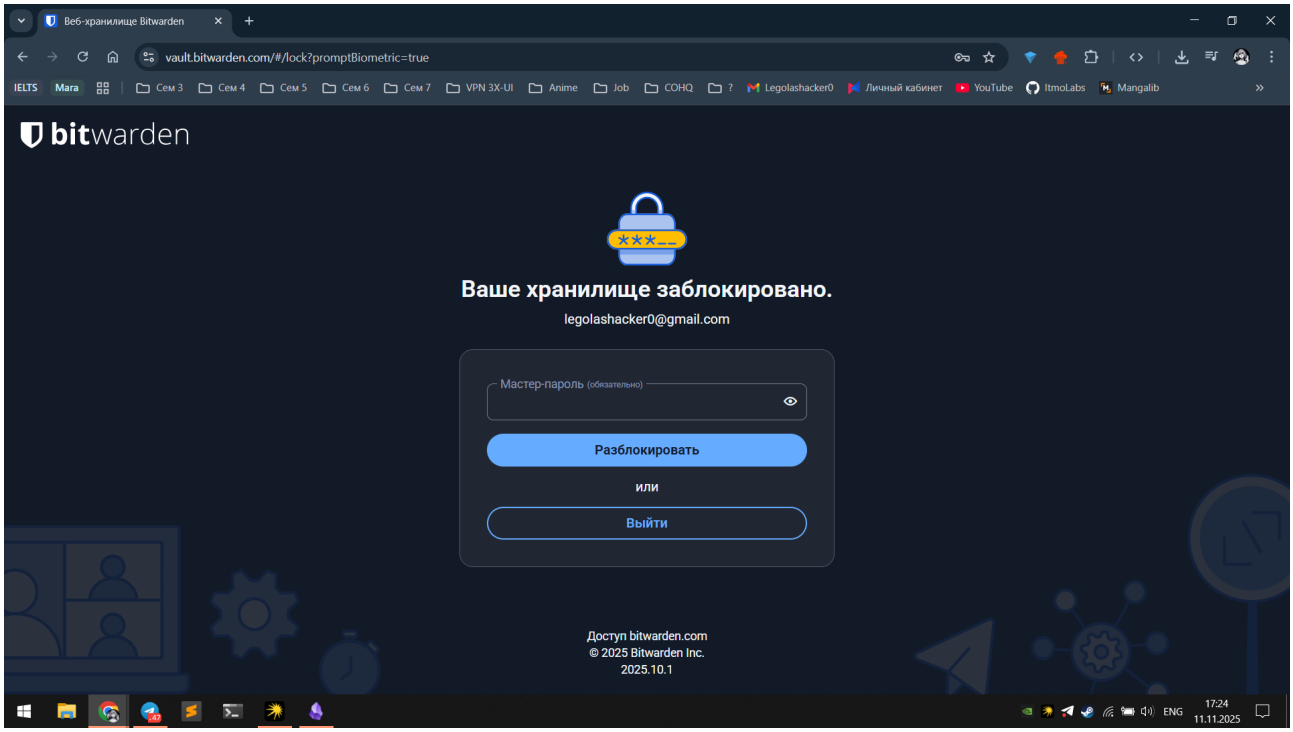

Рис. 1: Вход в учетную запись с мастер-паролем

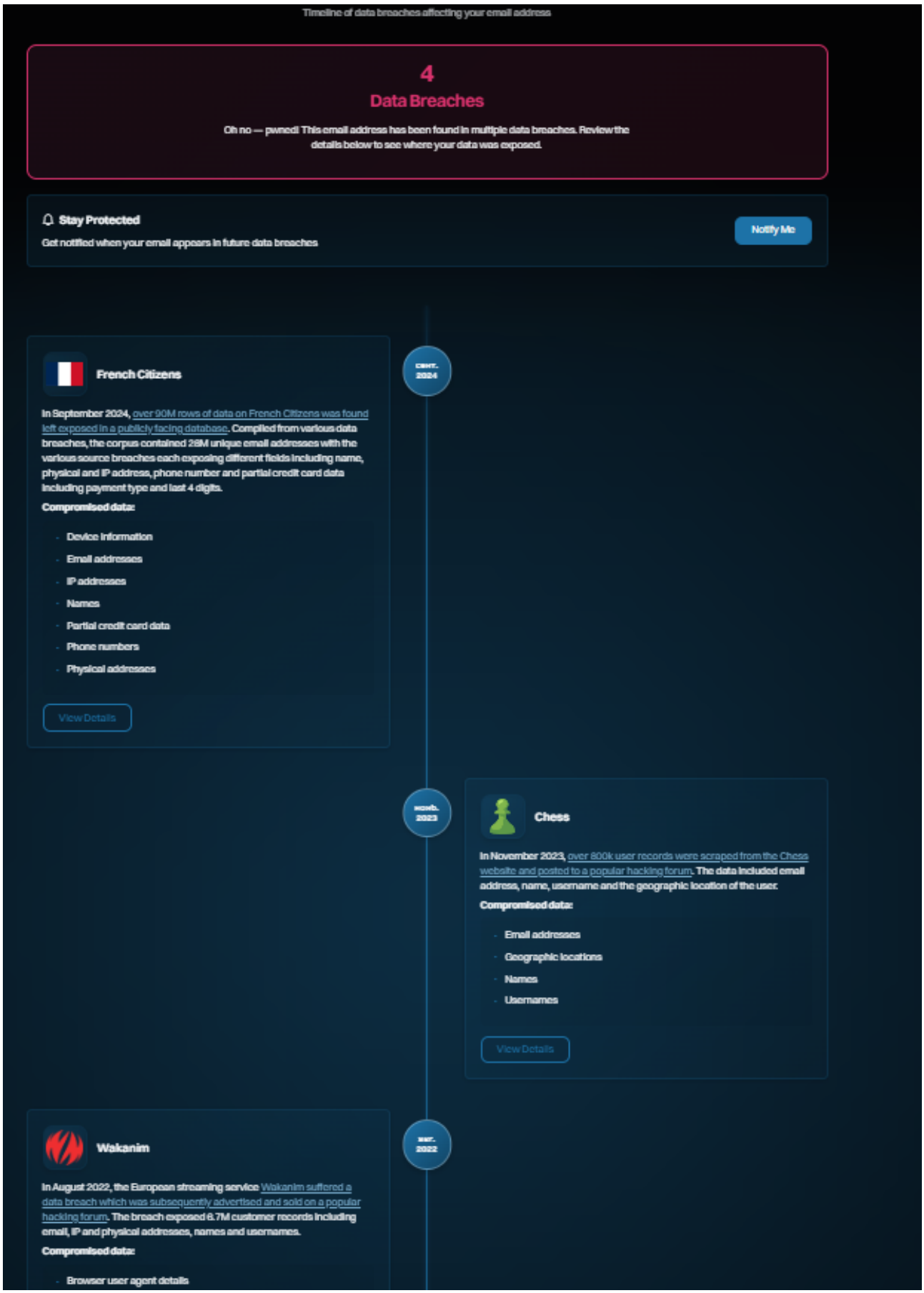

Рис. 2: Проверка почты на скомпрометированность

2 Аудит и замена паролей на надежные для 5 аккаунтов

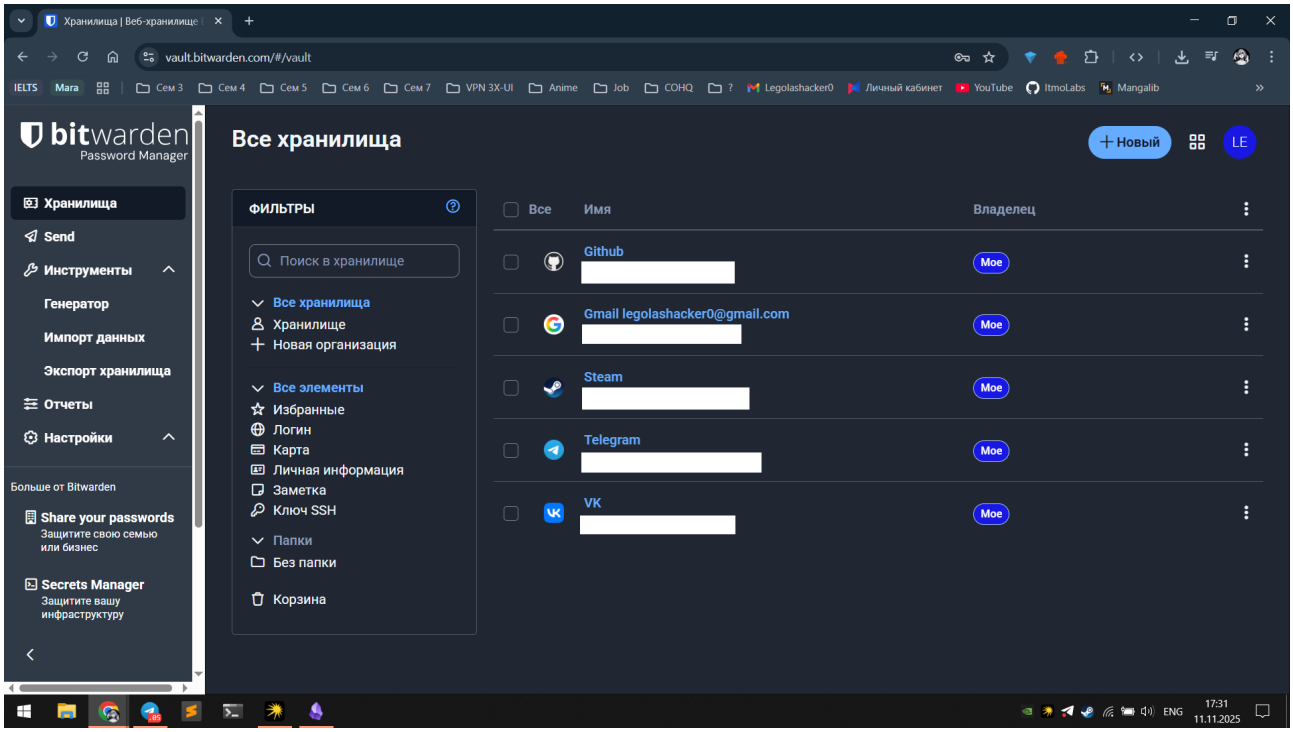

Рис. 3: Главный интерфейс менеджера паролей с созданной базой

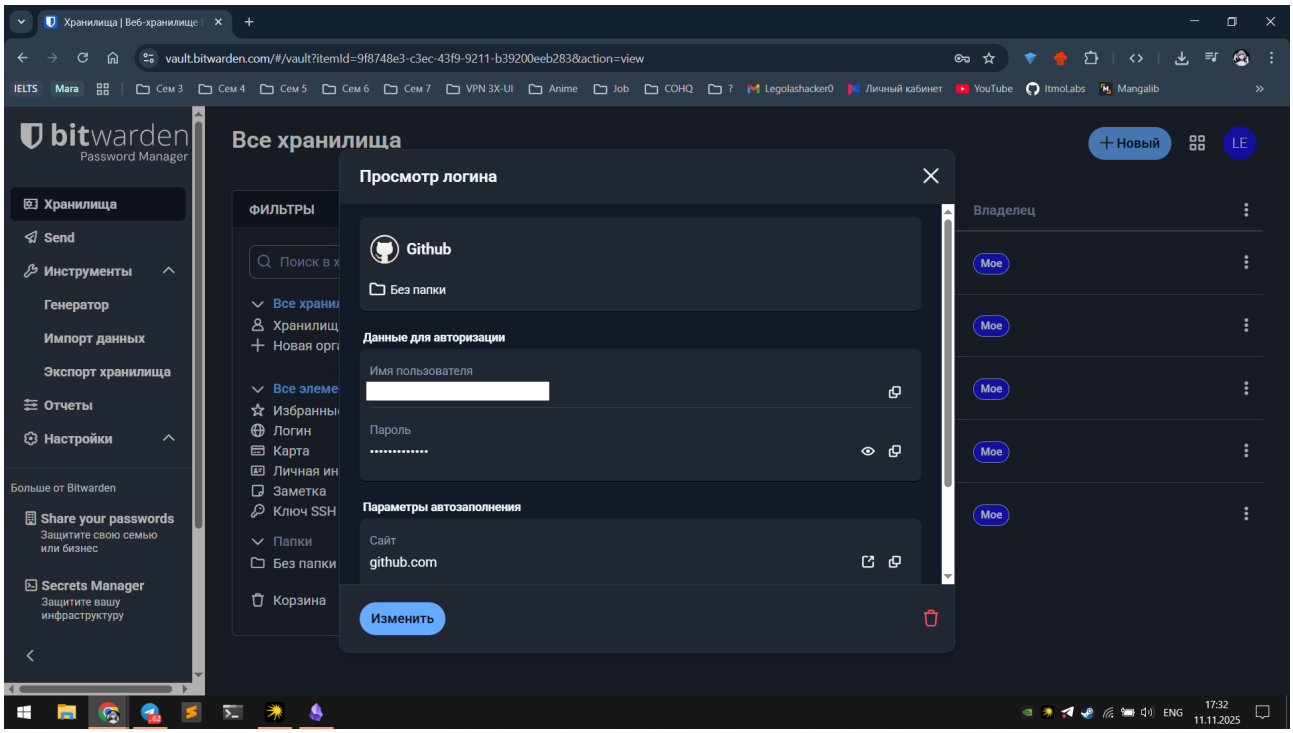

Рис. 4: Сгенерированные пароли

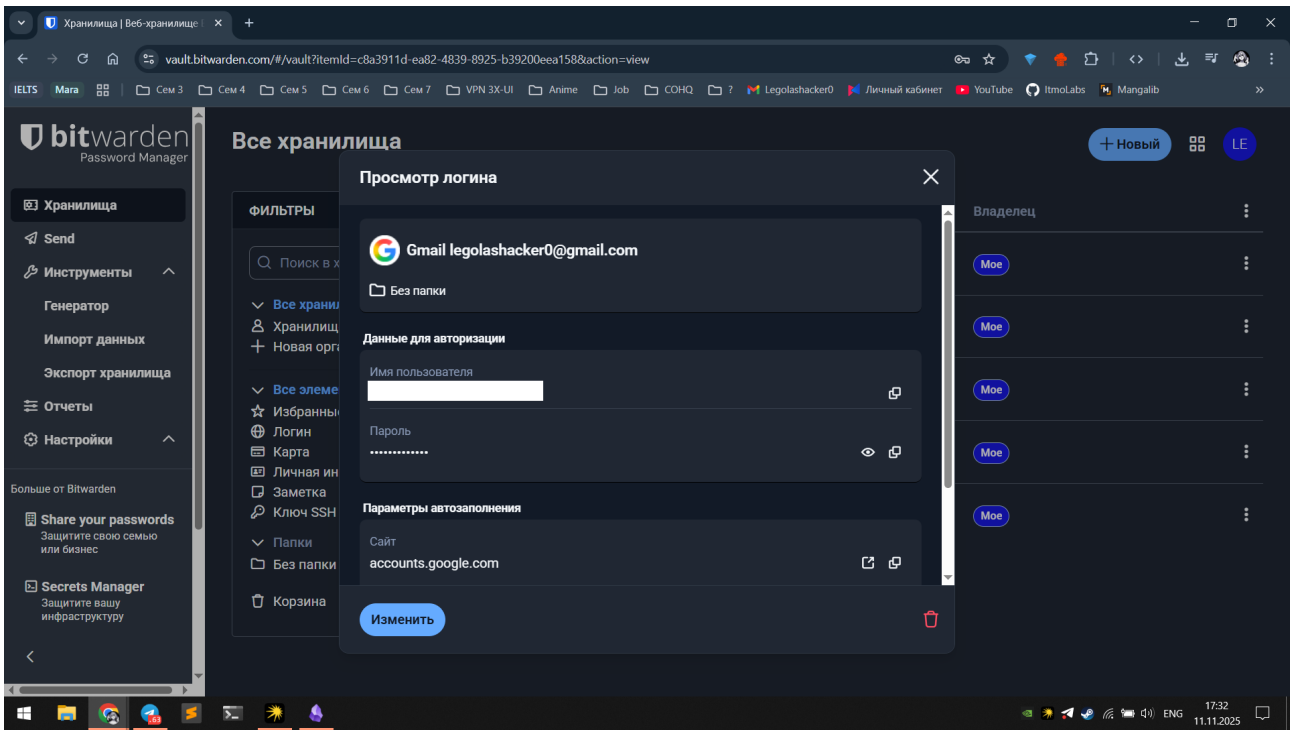

Рис. 5: Сгенерированные пароли

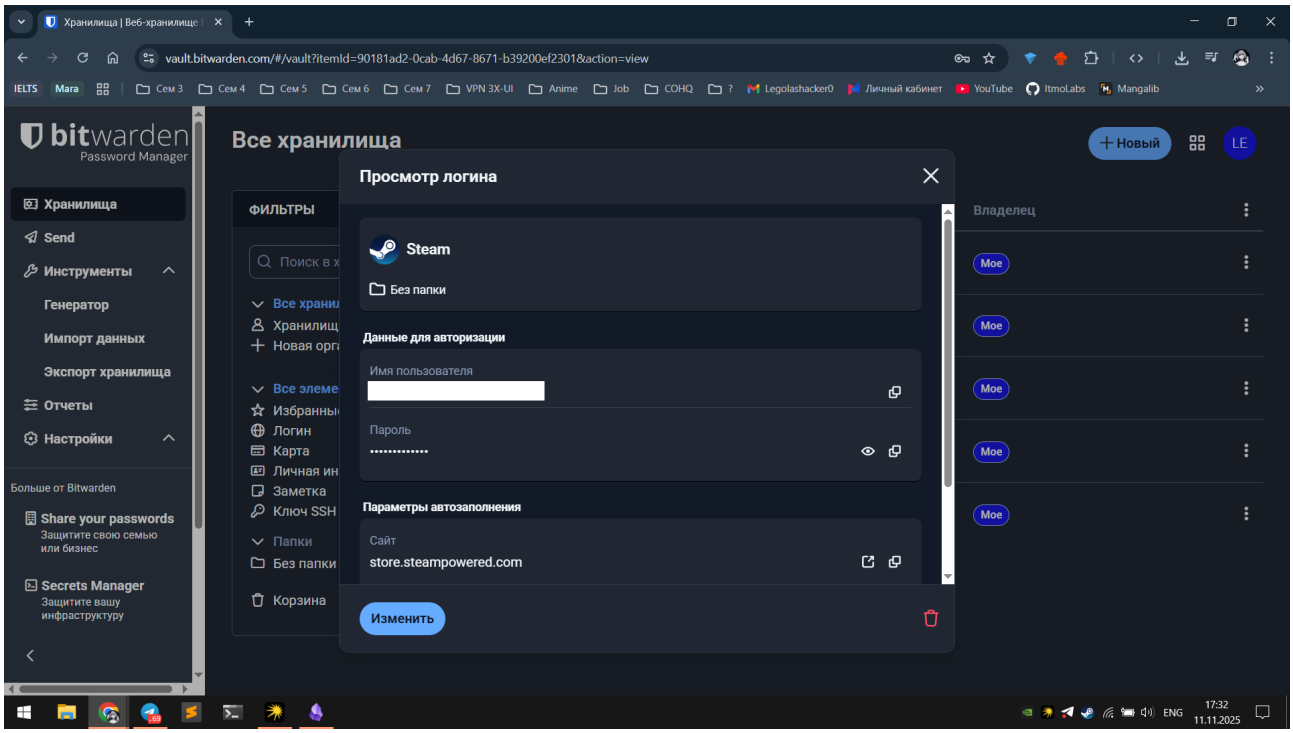

Рис. 6: Сгенерированные пароли

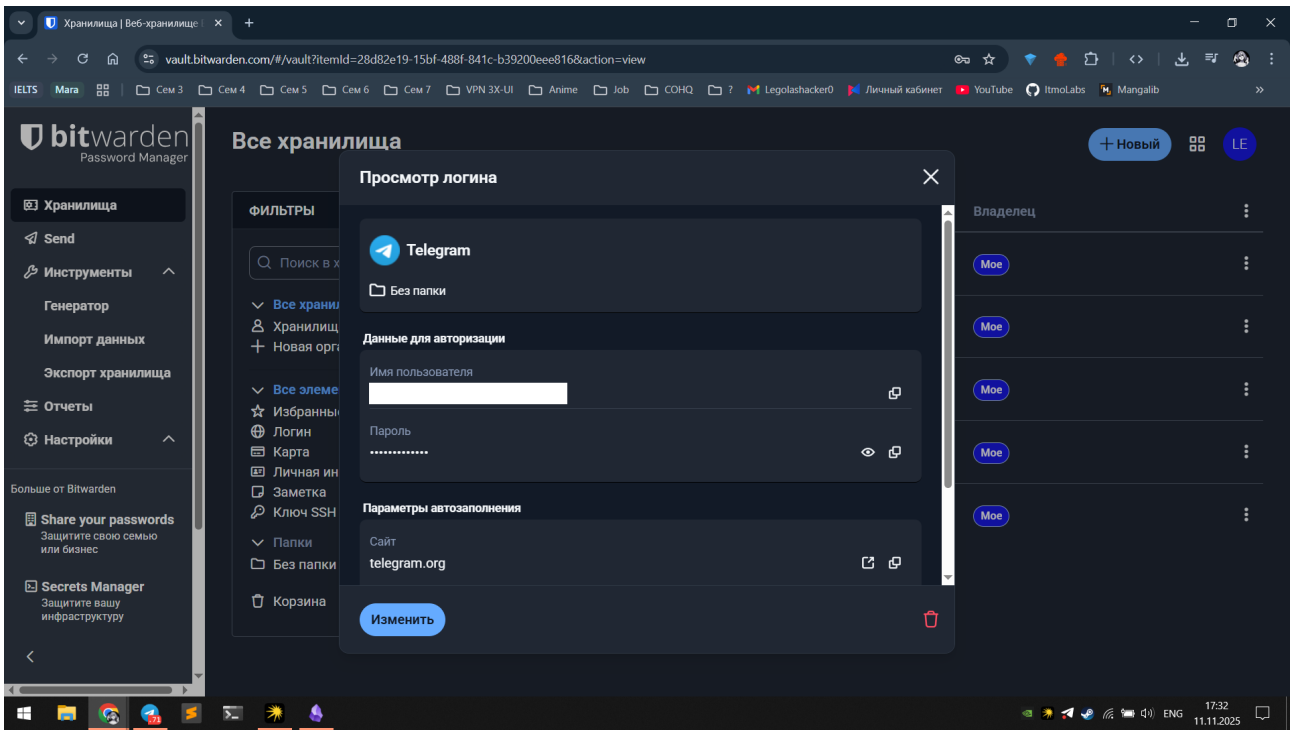

Рис. 7: Сгенерированные пароли

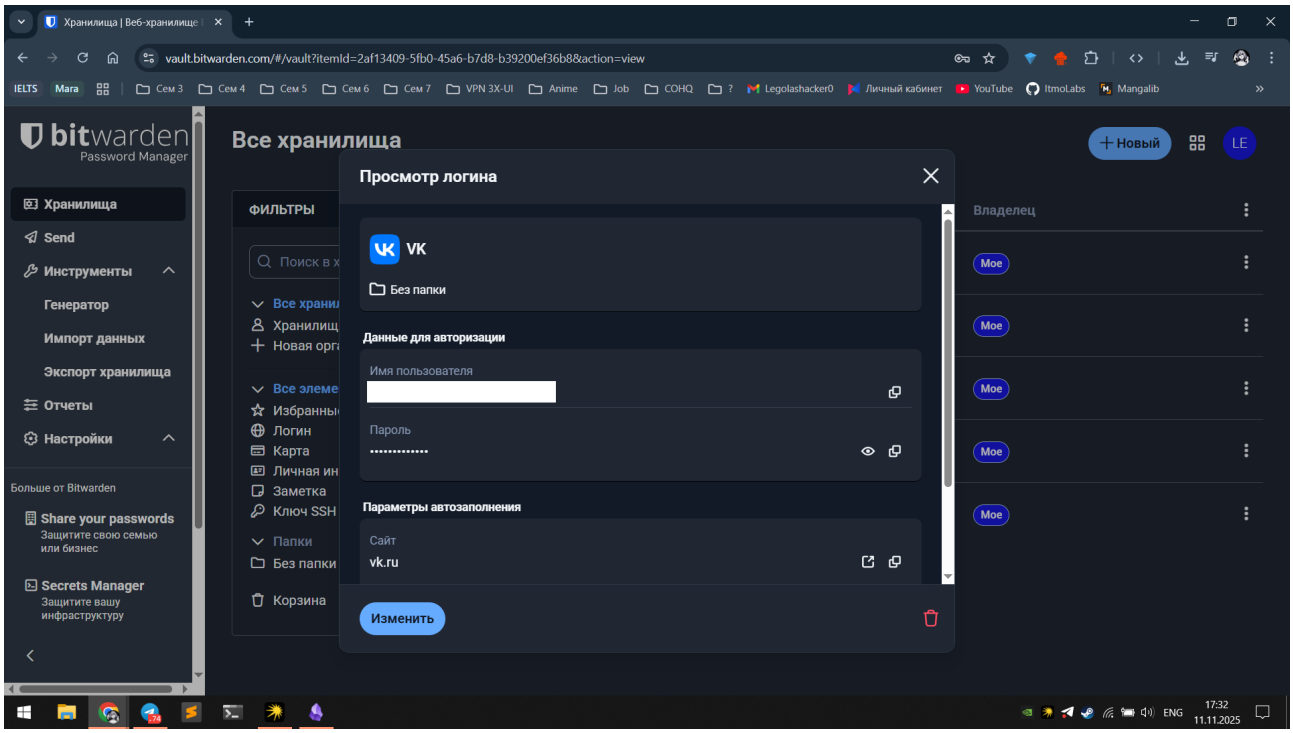

Рис. 8: Сгенерированные пароли

3 Настройка 2FA

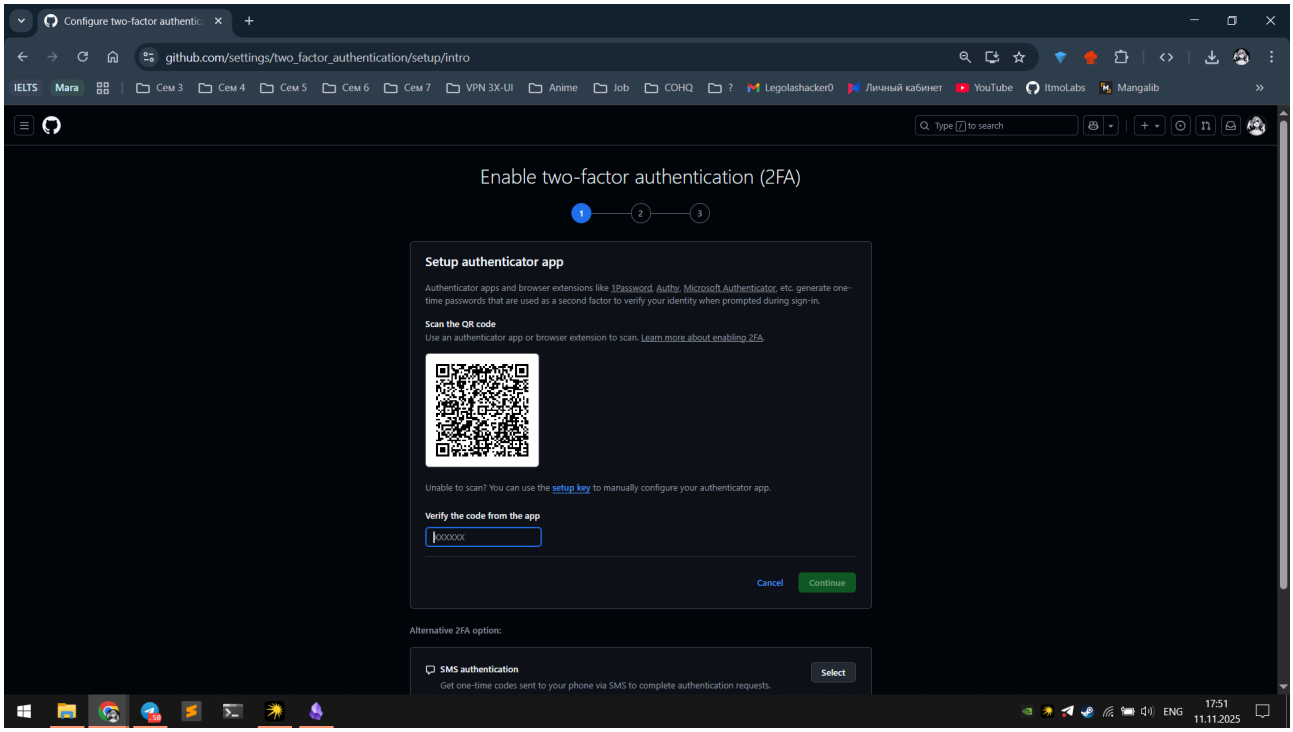

Рис. 9: Страница настройки двухфакторной аутентификации (2FA) для GitHub

17:52

49

Recently Deleted

GitHub

Last modified today

User Name	legolashacker0@gmail.com
Password	
Website	github.com

This password will be permanently deleted in 30 days unless it is recovered.

Recover

Delete

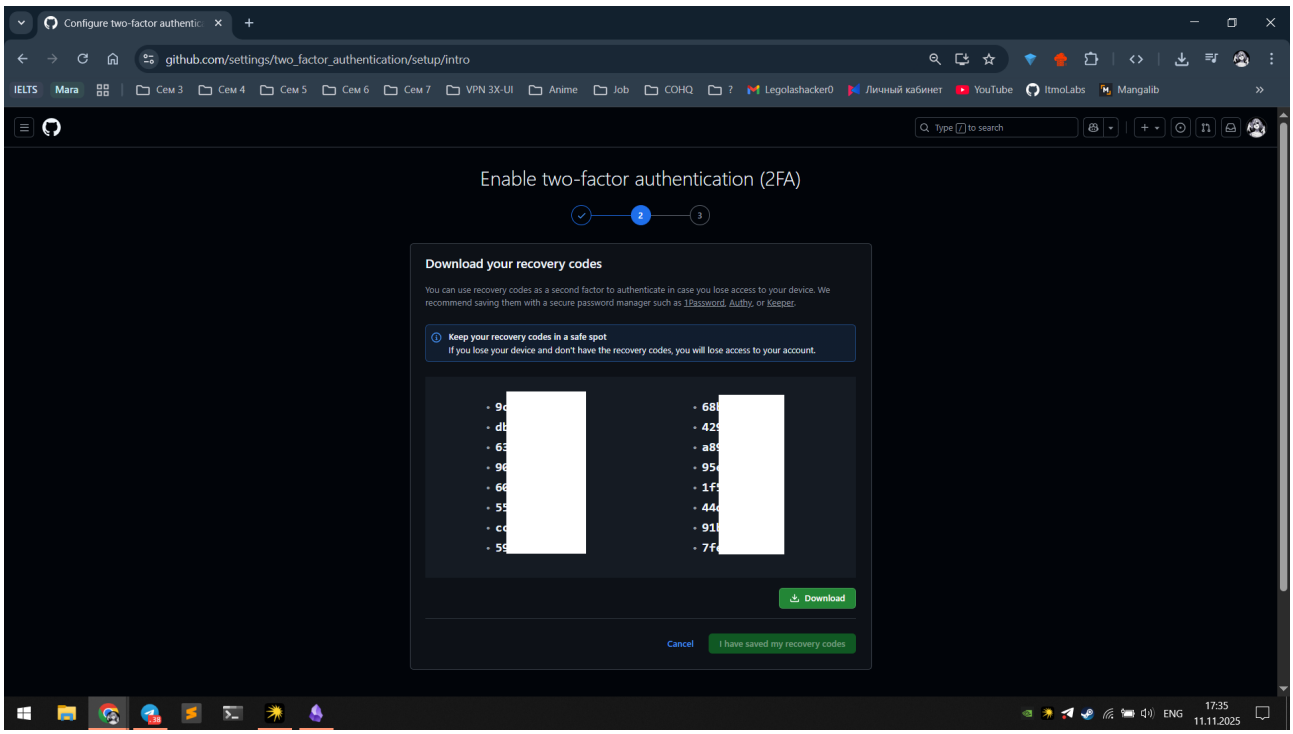

Рис. 11: Коды восстановления

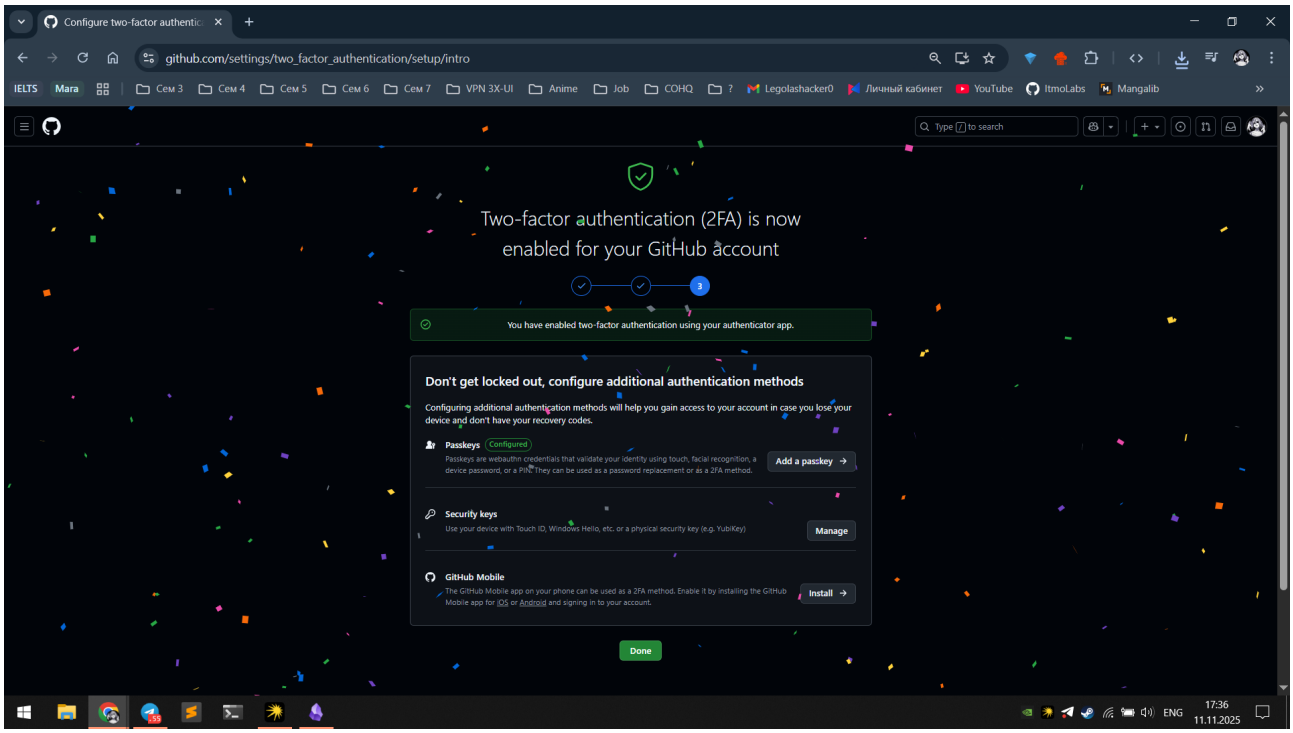

Рис. 12: Успешное создане 2FA Аутентификации

4 Ответы на вопросы

Мои аккаунты защищены всего двумя паролями: один состоит из 9 символов, другой из 10. Они различаются наличием специального символа и заглавной буквы, однако оба основаны на простых, легко угадываемых комбинациях. По этой причине мои пароли считаются слабыми и ненадёжными.

Двухфакторная аутентификация (2FA) - это метод повышения безопасности, при котором для входа в систему требуется не только пароль, но и дополнительное подтверждение личности. В качестве второго фактора могут использоваться SMS-код, отпечаток пальца, распознавание лица или одноразовый код из специального приложения.