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

Информационная безопасность

Работа №8

«Мини-исследование: Утечка данных и цифровая гигиена»

Барсуков Максим Андреевич

Группа: P3415

2025

Выполнение

Проверка email-адреса на наличие в утечках

Для проверки использовался сервис Have I Been Pwned (https://haveibeenpwned.com/). Был введён мой основной email-адрес: maximbarsukov@bk.ru. Как видно на рисунке 1, данные не были обнаружены в утечках.

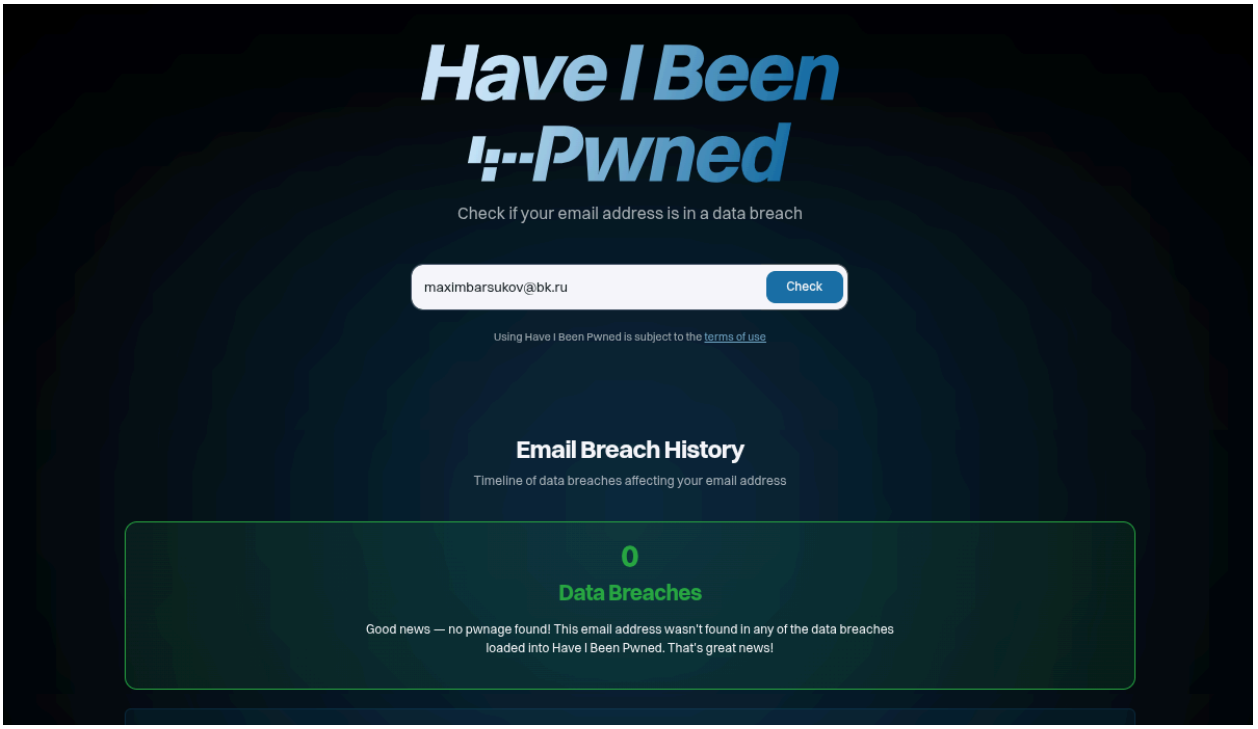

Рисунок 1 — Результаты проверки email-адреса в сервисе

Аудит публичных данных в социальных сетях

Проведен анализ профилей в следующих платформах:

1) ВКонтакте: публично доступны только фамилия и имя, видно подписки на группы, связанные с ИТМО (то есть можно предположить город и учебное заведение), как показано на рисунке 2.

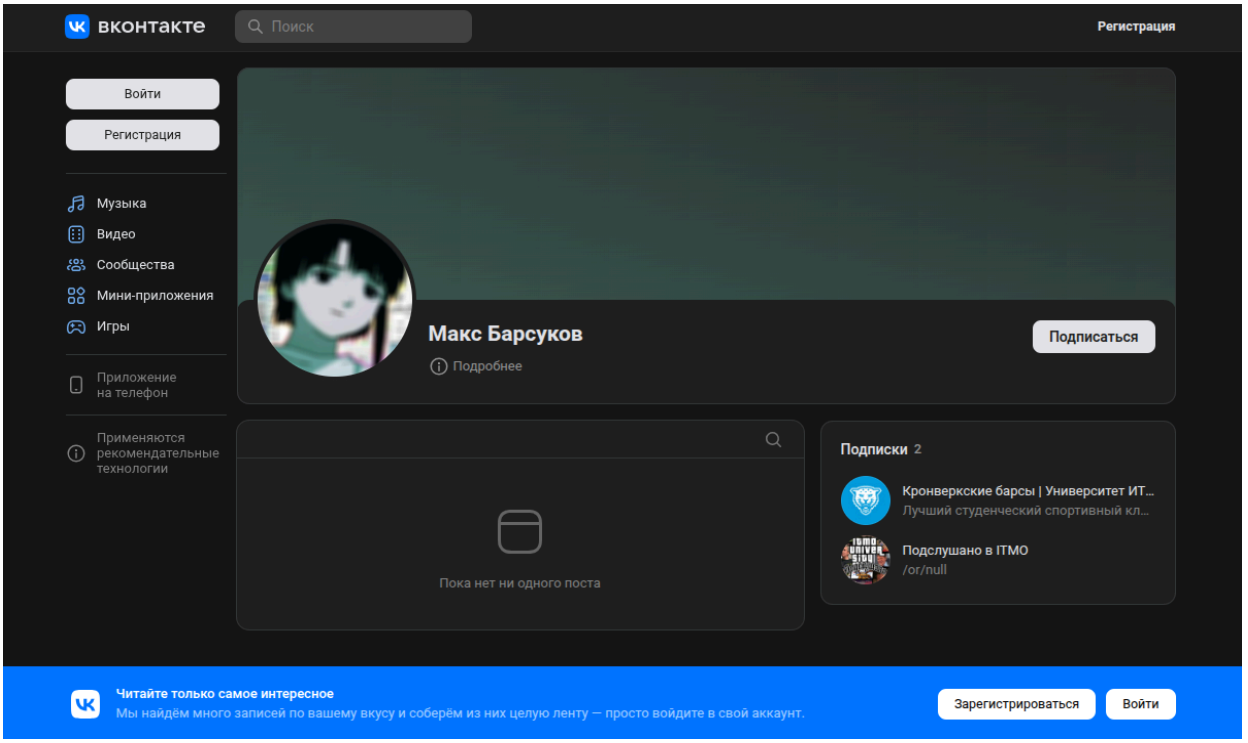

Рисунок 2 — Доступные данные на странице ВКонтакте

Никакие личные данные на странице не заполнены. Настройки приватности не позволяют незнакомцам просматривать список друзей.

2) Telegram: отображается имя, фамилия, никнейм и фото профиля, раздел «О себе» не заполнен. Номер телефона доступен только контактам, как показано на рисунке 3.

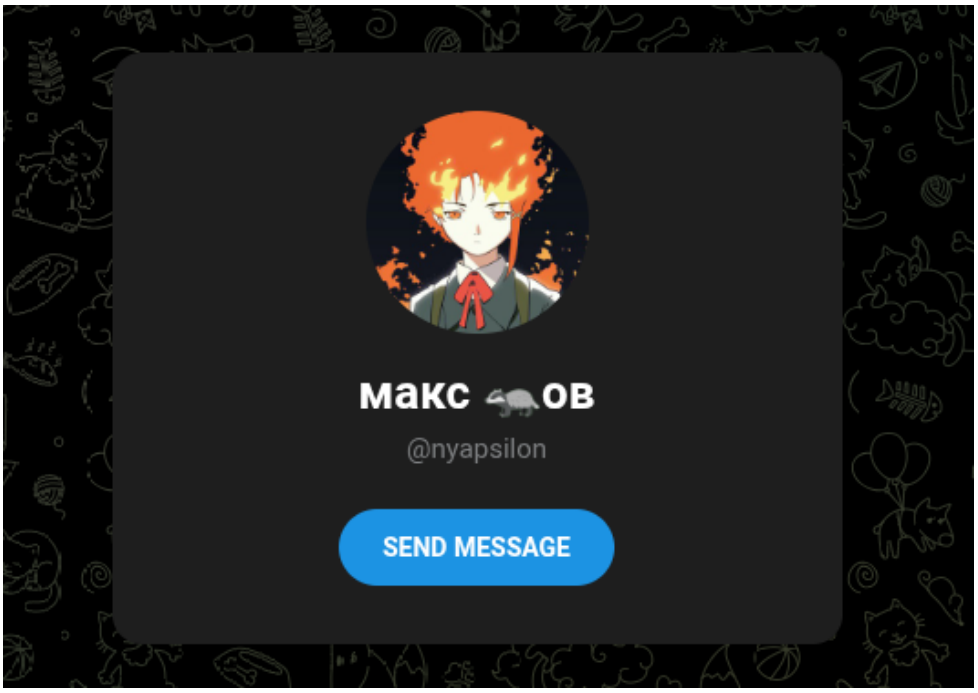

Рисунок 3 — Доступные данные для аккаунта в Telegram

Личные правила цифровой гигиены

На основе проведенного анализа сформулированы следующие правила:

1. Использовать уникальные сложные пароли для каждого сервиса и хранить их в менеджере паролей (например, Bitwarden).
2. Включить двухфакторную аутентификацию (2FA) на всех аккаунтах, поддерживающих эту функцию.
3. Раз в квартал проверять и корректировать настройки приватности в социальных сетях.
4. Не публиковать в открытом доступе информацию, которая может быть использована для восстановления доступа к аккаунтам (дата рождения, место учёбы, номер телефона).
5. Регулярно проверять, какие устройства и сессии авторизованы в ваших аккаунтах. Многие сервисы (Google, VK, Telegram, Apple ID и др.) позволяют просматривать активные сессии. Раз в месяц заходить в настройки безопасности и завершать подозрительные или устаревшие сеансы.
6. Ограничить использование геолокации в приложениях и соцсетях. Отключить геотеги в фото и не публиковать посты с точным местоположением в реальном времени — это снижает риски физического преследования, кражи или социальной инженерии.