

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

«Информационная безопасность»

Работа 5: Аудит паролей с помощью менеджера паролей

Выполнил:

Румский Александр Максимович

Группа:

P3407

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург, 2025 год

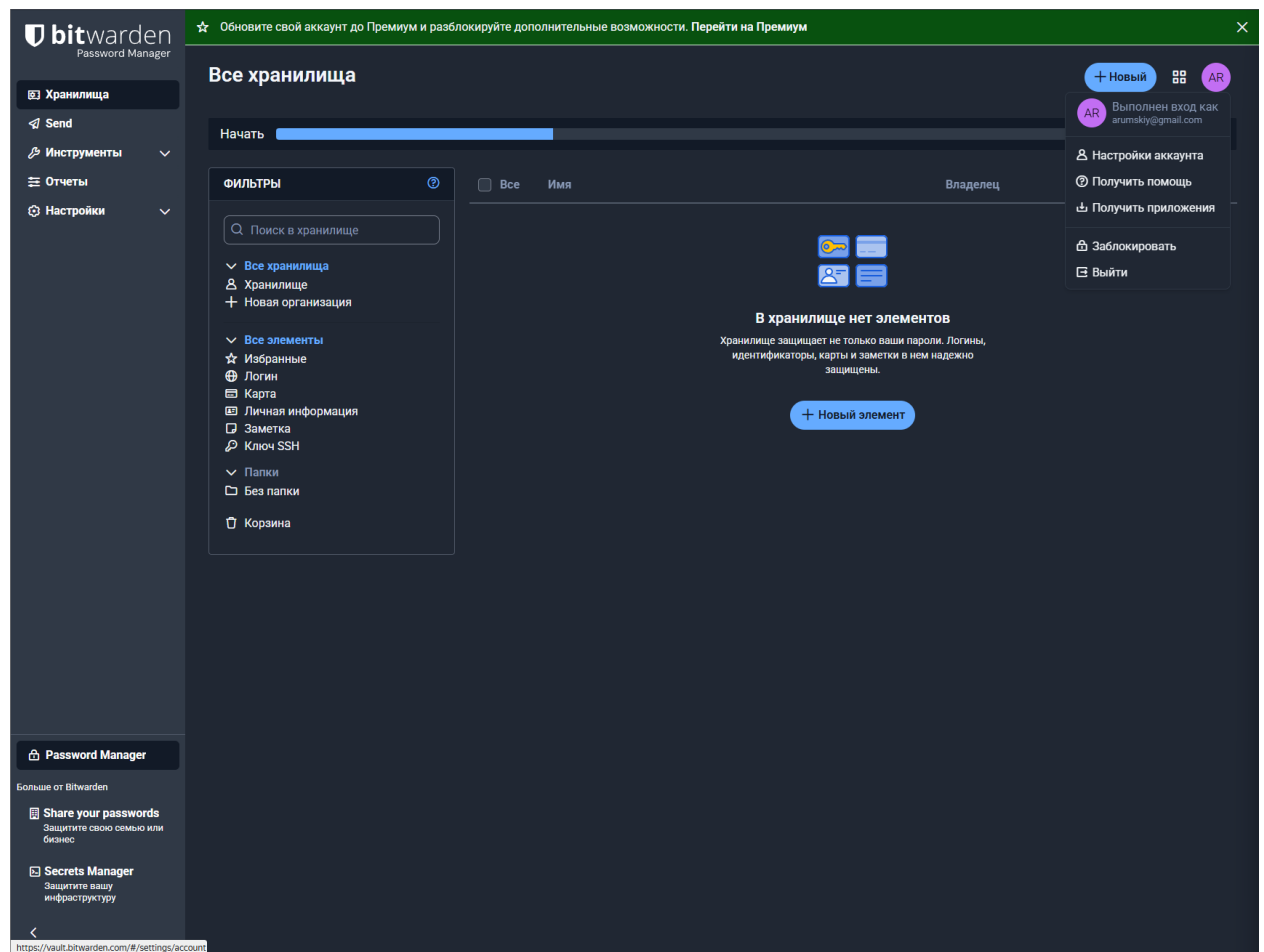
Содержание

Регистрация в bitwarden	3
Проверка утечек	4
Генерация паролей.....	6
Microsoft.....	6
Gmail.....	7
NexusMods	8
4pda	9
GitHub	10
Итог.....	11
Двухфакторная аутентификация.....	12
Ответы на вопросы	15
Какие пароли были слабыми	15
Что такое 2FA.....	15

Регистрация в bitwarden

Мастер-пароль был сгенерирован с помощью сервиса

<https://password.kaspersky.com/ru/>



Проверка утечек

Сайт <https://haveibeenpwned.com/> показал следующее

The screenshot shows the Have I Been Pwned website interface. At the top, there is a navigation bar with links: Who's Been Pwned, Passwords, Notify Me, API, Demos, Pricing, About, and a Dashboard button. The main heading reads "Have I Been Pwned" with the tagline "Check if your email address is in a data breach". Below this, a search bar contains the email "arumskiy@gmail.com" and a "Check" button. A small note states: "Using Have I Been Pwned is subject to the [terms of use](#)".

The "Email Breach History" section shows a "Timeline of data breaches affecting your email address". A large red box displays the result: "12 Data Breaches". Below this, a message reads: "Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed."

Из них 3 последние утечки произошли 03.22, 08.24 и 02.25

Последняя:

This screenshot shows a detailed view of a data breach entry. On the left, a circular badge indicates the date "февр. 2025". The main section is titled "ALIEN TXTBASE Stealer Logs" with a document icon. The text describes the breach: "In February 2025, 23 billion rows of stealer logs were obtained from a Telegram channel known as ALIEN TXTBASE. The data contained 284M unique email addresses alongside the websites they were entered into and the passwords used. This data is now searchable in HIBP by both email domain and the domain of the target website."

Under the heading "Compromised data:", there is a list of affected data types:

- Email addresses
- Passwords

A "View Details" button is located at the bottom of the entry.

Генерация паролей

Microsoft

Новый логин

Информация об элементе

Название элемента (обязательно)
Microsoft

Папка
Без папки

Данные для входа

Имя пользователя
agums

Пароль

Использовать

Ключ доступа

Параметры

Сайт (URL)
https://

+ Добавить

Дополнительно

Заметки

☐ Повторный запрос мастер-пароля

+ Добавить поле

Сохранить

Отмена

Генератор паролей

Пароль

Парольная фраза

Пароль

Парольная фраза

Опции

Длина
16
Значение должно быть между 9 и 128.

Включить

☒ A-Z ☒ a-z ☒ 0-9 ☒ !@#\$%^&*

Минимум цифр
4

Минимум символов
3

☐ Избегать неоднозначных символов

Использовать этот пароль

Новый логин

Информация об элементе

Название элемента (обязательно)
gmail

Папка
Без папки

Данные для входа

Имя пользователя
arums

Пароль
.....

Использовать пароль

Ключевая фраза

Параметры

Сайт (URL)
https://

+ Добавить

Дополнительно

Заметки

Повторный запрос мастер-пароля

+ Добавить поле

Сохранить

Отмена

Генератор паролей

Пароль

Парольная фраза

.....

↺

📋

Опции

Длина
16
Значение должно быть между 9 и 128.

Включить

☒ A-Z

☒ a-z

☒ 0-9

☒ !@#\$%^&*

Минимум цифр
4

Минимум символов
3

☐ Избегать неоднозначных символов

Использовать этот пароль

Новый логин

Информация об элементе

Название элемента (обязательно)
NexusMods

Папка
Без папки

Данные для входа

Имя пользователя
ХотТай

Пароль
.....

Безопасность

Ключевые слова

Параметры

Сайт (URL)
https://

+ Добавить

Дополнительно

Заметки

☐ Повторный запрос мастер-пароля

+ Добавить поле

Сохранить

Отмена

Генератор паролей

Пароль

Парольная фраза

.....

↺

📋

Опции

Длина
16
Значение должно быть между 9 и 128.

Включить

☒ A-Z ☒ a-z ☒ 0-9 ☒ !@#\$%^&*

Минимум цифр
4

Минимум символов
3

☐ Избегать неоднозначных символов

Использовать этот пароль

Новый логин

Информация об элементе

Название элемента (обязательно)

4PDA

Папка

Без папки

Данные для входа

Имя пользователя

agims

Пароль

Использовать мастер-пароль

Ключ доступа

Параметры

Сайт (URL)

https://

+ Добавить

Дополнительно

Заметки

Повторный запрос мастер-пароля

+ Добавить поле

Сохранить

Отмена

Генератор паролей

Пароль

Парольная фраза

Опции

Длина

16

Значение должно быть между 9 и 128.

Включить

☒ A-Z

☒ a-z

☒ 0-9

☒ !@#\$%^&*

Минимум цифр

4

Минимум символов

3

☐ Избегать неоднозначных символов

Использовать этот пароль

Новый логин

Информация об элементе

Название элемента (обязательно)
GitHub

Папка
Без папки

Данные для входа

Имя пользователя
agum...

Пароль

Использовать

Ключ

Параметры

Сайт (URL)
https://

+ Добавить

Дополнительно

Заметки

☐ Повторный запрос мастер-пароля

+ Добавить поле

Сохранить

Отмена

Генератор паролей

Пароль

Парольная фраза

Опции

Длина
16
Значение должно быть между 9 и 128.

Включить
☒ A-Z ☒ a-z ☒ 0-9 ☒ !@#\$%^&*
Минимум цифр 4
Минимум символов 3
☐ Избегать неоднозначных символов

Использовать этот пароль

bitwarden

Password Manager

Хранилища

Send

Инструменты

Отчеты

Настройки

Password Manager

Больше от Bitwarden

Share your passwords

Защитите свою семью или бизнес

Secrets Manager

Защитите вашу инфраструктуру

Обновите свой аккаунт до Премиум и разблокируйте дополнительные возможности. Перейти на Премиум

Все хранилища

+ Новый

AR

Начать

✓ Создать аккаунт

✓ Импортировать данные

Установить расширение для браузера

Выполнено 2/3

Фильтры

Поиск в хранилище

Все хранилища

Хранилище

Новая организация

Все элементы

Избранные

Логин

Карта

Личная информация

Заметка

Ключ SSH

Папки

Без папки

Корзина

Все

Имя

Владелец

4PDA

Moe

GitHub

Moe

gmail

Moe

Microsoft

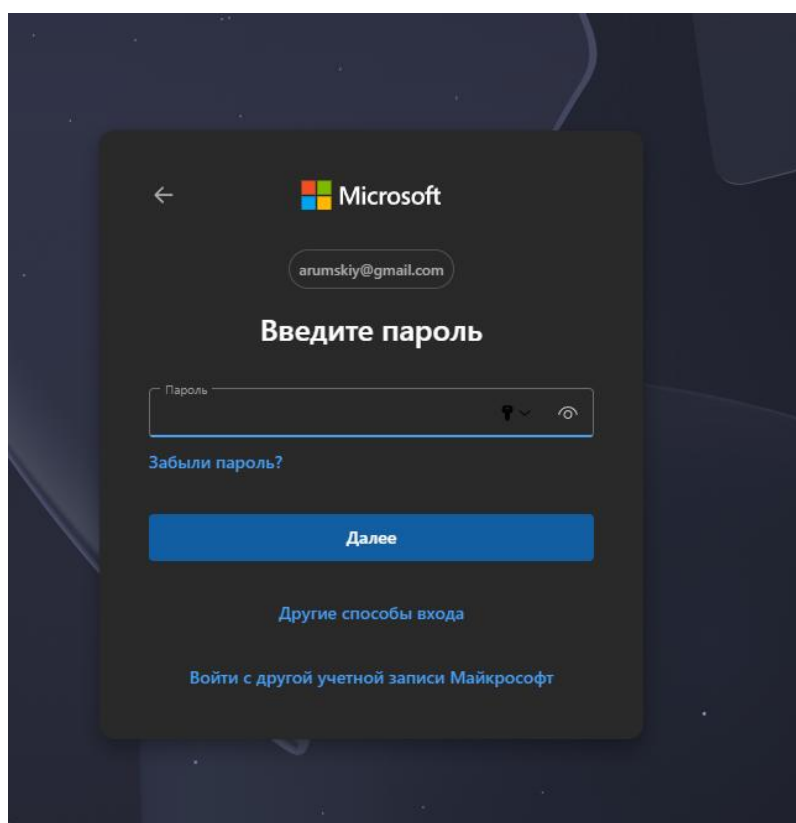
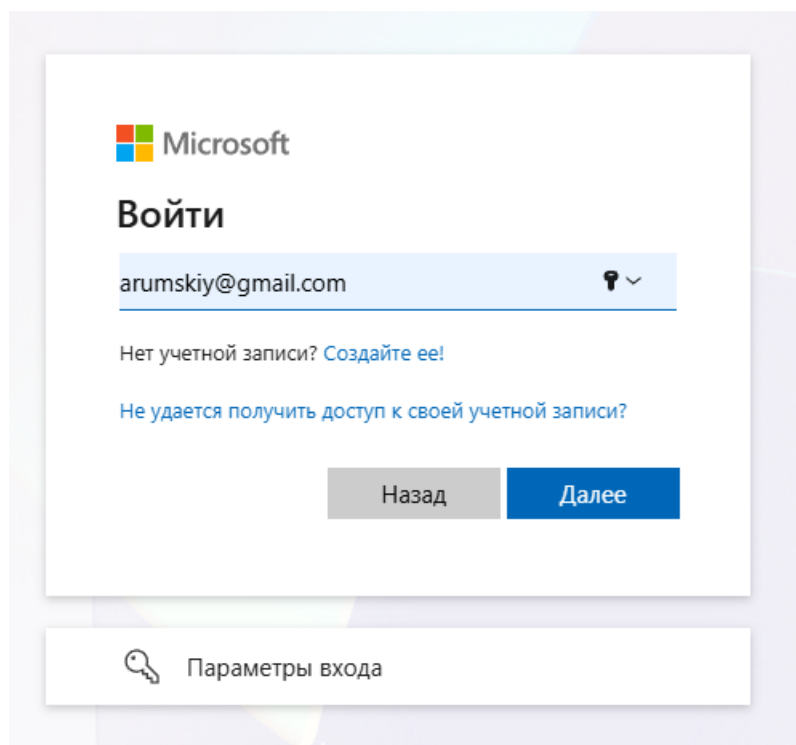
Moe

NexusMods

Moe

Двухфакторная аутентификация

Двухфакторная аутентификация настроена для аккаунта Microsoft, через их приложение Authenticator для мобильных устройств. Приложение не позволяет делать скриншоты своего интерфейса, так что могу приложить только порядок входа. Ввожу логин и пароль, получаю запрос на подтверждение





arumskiy@gmail.com

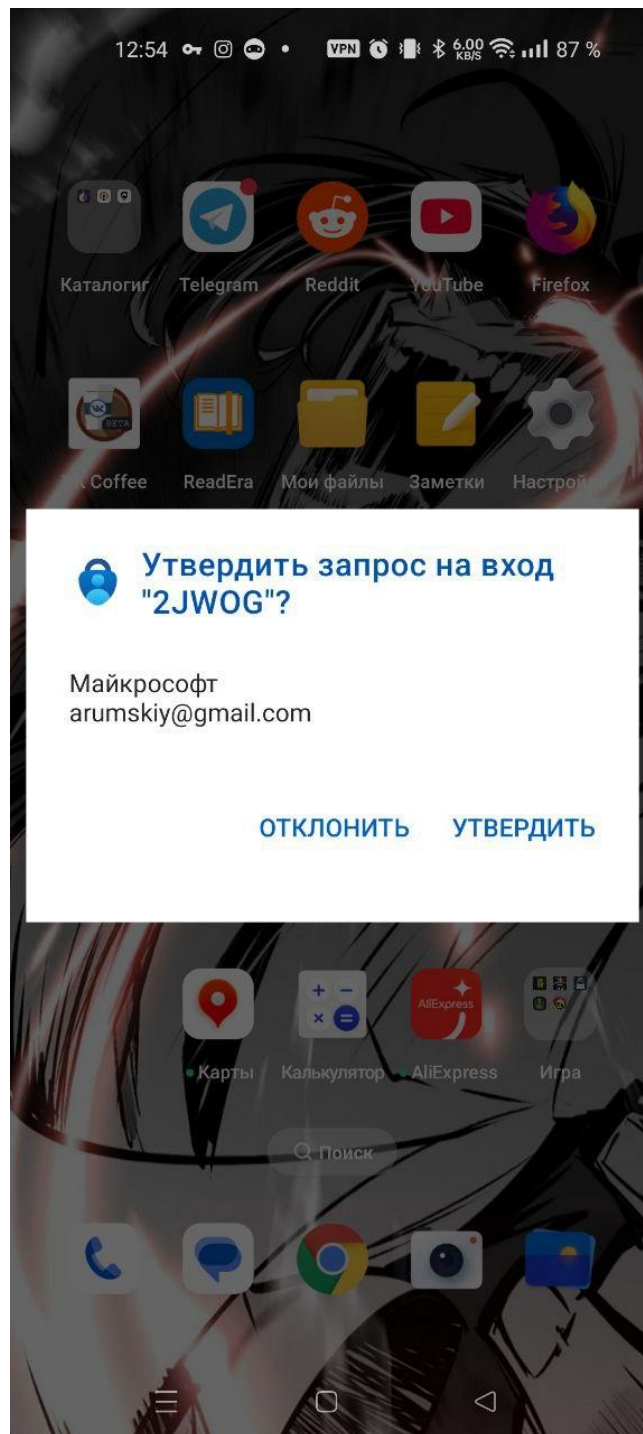
Утвердить запрос на вход



Утвердите запрос 2JWOG в приложении Microsoft Authenticator для доступа к конфиденциальной информации.

☒ Больше не спрашивать на этом устройстве

[Другие способы входа](#)



После получения уведомления на телефоне и подтверждения отпечатком пальца, происходит вход в аккаунт Microsoft

Ответы на вопросы

Какие пароли были слабыми

Слабыми оказались пароли, которые я использовал для сервисов, которыми пользуюсь чаще всего, так как в них время от времени приходится входить заново (из-за истечения срока годности токенов доступа), и со временем, ввиду повторяющейся время от времени процедуры восстановления паролей, они становились всё проще. Стали содержать меньше спец. символов/цифр, остались только одна-две заглавные буквы.

Что такое 2FA

2FA – 2-Factor Authentication – двухфакторная аутентификация. Это механизм, добавляющий второй слой защиты аккаунта, помимо пароля. С включенной 2FA вы не сможете зайти в свой аккаунт, используя только пароль. Она может срабатывать как на попытки входа из новых мест/ с новых устройств, так и на постоянной основе(зависит от конкретного сайта/приложения). Работает она просто – после ввода корректного пароля, от пользователя требуют подтвердить вход одним из нескольких способов. Это может быть ввод кода из SMS/звонка, переход по ссылке с почты или подтверждение в приложении-аутентификаторе. Данный шаг позволяет защитить аккаунт от несанкционированного доступа третьими лицами, не обладающими доступом к второму фактору защиты пользователя.