Федеральное государственное автономное

образовательное учреждение высшего образования

 «Национальный исследовательский университет ИТМО»

**Информационная безопасность**

**Работа №5**

**«Аудит паролей с помощью менеджера паролей»**

Текст — Менять на свою

Текст — Лучше менять, чтобы не было вопросов по поводу антиплагиата

Текст — Выбрать один из вариантов

Фамилия Имя Отчество

Группа: P34XX

202X

# **Выполнение**

## Создание и настройка менеджера паролей

Для настройки BitWarden сначала нужно было создать учетную запись, поэтому для этого указана почта (рисунок 1).



Рисунок 1 — Ввод электронной почты для создания учетной записи

После ввода почты на форму пришло письмо со ссылкой для активации учетной записи, как показано на рисунке 2.



Рисунок 2 — Ввод хорошей мастер-пароли для создания учетной записи

Переходя по этой ссылке, появилась форма, куда нужно было вводить мастер-пароль. На рисунке 3 показано, как этот шаг был произведен.



Рисунок 3 — Ввод хорошей мастер-пароли для создания учетной записи

После успешного создания учетной записи было произведено скачивание BitWarden. После выборы опции установка (как показано на рисунке 4) успешно произведено скачивание (рисунок 5).



Рисунок 4 — Конфигурация режима установки BitWarden



Рисунок 5 — Окончание установки BitWarden

И после последующей аутентификации с помощью данных учётной записи, созданного заранее, было полностью сконфигурирована BitWarden на персональном компьютере. Рисунок 6 — подтверждение.



Рисунок 6 — настроенное приложение BitWarden на ПК

## Аудит и замена паролей на надежные для 5 аккаунтов

Проведен анализ паролей в следующих платформах:

1) Платформа/сайт №1:



Рисунок 7 — Данные аутентификации для сайта ...

Анализ устойчивости пароли: писать про используемый набор символов в пароли, длина пароли, присутствие словарных слов и распространённых паттернов на клавиатуре (qwerty), либо последовательностей (123 или abc), а также уникальности пароля среди других в вашем распоряжении.

Если не скомпрометированы: приложить скрин из haveibeenpwned.com с сайтами, которые содержат утечки ваших данных. Если ничего нет, то приложить скрин с отсутствием утечек.

Данные из этого сайта не были скомпрометированы. То, что были — показаны на рисунке 8.

Если скомпрометированы: приложить скрин из haveibeenpwned.com с этим сайтом (!), в котором описаны все проблемы.

Данные из этого сайта были скомпрометированы. На рисунке 8 (!) показаны все детали этой утечки данных.



Рисунок 8 — Сайт(ы) с скомпрометированными данными/Отсутствие скомпрометированных данных

2) Платформа/сайт №2:



Рисунок 9 — Данные аутентификации для сайта ...

Анализ устойчивости пароли: писать про используемый набор символов в пароли, длина пароли, присутствие словарных слов и распространённых паттернов на клавиатуре (qwerty), либо последовательностей (123 или abc), а также уникальности пароля среди других в вашем распоряжении.

Если не скомпрометированы: не приложить скрин, оставить только текст ниже.

Данные из этого сайта не были скомпрометированы.

Если скомпрометированы: приложить скрин из haveibeenpwned.com с этим сайтом (!), в котором описаны все проблемы.

Данные из этого сайта были скомпрометированы. На рисунке 10 (!) показаны все детали этой утечки данных.



Рисунок 10 — Сайт с скомпрометированными данными

3) Платформа/сайт №3:



Рисунок 11 — Данные аутентификации для сайта ...

Анализ устойчивости пароли: писать про используемый набор символов в пароли, длина пароли, присутствие словарных слов и распространённых паттернов на клавиатуре (qwerty), либо последовательностей (123 или abc), а также уникальности пароля среди других в вашем распоряжении.

Если не скомпрометированы: не приложить скрин, оставить только текст ниже.

Данные из этого сайта не были скомпрометированы.

Если скомпрометированы: приложить скрин из haveibeenpwned.com с этим сайтом (!), в котором описаны все проблемы.

Данные из этого сайта были скомпрометированы. На рисунке 12 (!) показаны все детали этой утечки данных.



Рисунок 12 — Сайт с скомпрометированными данными

4) Платформа/сайт №4:



Рисунок 13 — Данные аутентификации для сайта ...

Анализ устойчивости пароли: писать про используемый набор символов в пароли, длина пароли, присутствие словарных слов и распространённых паттернов на клавиатуре (qwerty), либо последовательностей (123 или abc), а также уникальности пароля среди других в вашем распоряжении.

Если не скомпрометированы: не приложить скрин, оставить только текст ниже.

Данные из этого сайта не были скомпрометированы.

Если скомпрометированы: приложить скрин из haveibeenpwned.com с этим сайтом (!), в котором описаны все проблемы.

Данные из этого сайта были скомпрометированы. На рисунке 14 (!) показаны все детали этой утечки данных.



Рисунок 14 — Сайт с скомпрометированными данными

5) Платформа/сайт №5:



Рисунок 15 — Данные аутентификации для сайта ...

Анализ устойчивости пароли: писать про используемый набор символов в пароли, длина пароли, присутствие словарных слов и распространённых паттернов на клавиатуре (qwerty), либо последовательностей (123 или abc), а также уникальности пароля среди других в вашем распоряжении.

Если не скомпрометированы: не приложить скрин, оставить только текст ниже.

Данные из этого сайта не были скомпрометированы.

Если скомпрометированы: приложить скрин из haveibeenpwned.com с этим сайтом (!), в котором описаны все проблемы.

Данные из этого сайта были скомпрометированы. На рисунке 16 (!) показаны все детали этой утечки данных.



Рисунок 16 — Сайт с скомпрометированными данными

Для того, чтобы все пароли вышеперечисленных платформ были адекватными с точки зрения стойкости, требуется их полная замена на пароли, соответствующих следующим требованиям:

* Использование символов из максимально возможных видов. Сюда входят заглавные и строчные латинские буквы, цифры и специальные символы (“!”, “#”, “%”, “@”, “$” и т.д.).
* Избежание использования пароля длиной менее 16 символов.
* Избежание переиспользования одного и того же пароля на разных платформах.
* Рандомизирование содержания пароля до максимальной степени. Не допускается использование словарных слов, публично известных фактов, личной информации (имя, день рождения, телефон и т.д.) и широкораспространённых последовательностей символов (123456789, qwerty и т.д.).
* Избежание использования пароля, обнаруженных в публичных утечках данных.

Производим этого на практике. Для этого в BitWarden надо добавить запись с данными аутентификации. Форма для этого показана на рисунке 13.



Рисунок 17 — Форма для создания записи в «BitWarden»

Для того, чтобы произвести пароля, соответствующая вышеперечисленным требованиям, можно надать на специальную кнопку генерации. Там возможно настраивать нового пароля под своим требованиям, как показано на рисунке 18.



Рисунок 18 — Форма с параметрами для создания нового пароля в «BitWarden»

Были произведены аналогичные шаги со всеми записями, итого которых показана на рисунке 15.



Рисунок 19 — записи в «BitWarden» аккаунтов с новыми паролями

## Подключение 2FA через ТОТР

Одного пароля обычно не хватит для беопасности. Надо ещё рассматривать сценарию, когда пароль каким-то образом оказалась у потенциального злоумышленника.

Для этого был придуман двухфакторная аутентификация, который дает доступ пользователю только после предоставления двух или более видов «доказательства механизма аутентификации». К ним обычно относят:

* Знание: пароля, ПИН-код, ключевая фраза и т.д.
* Владение: электронная или магнитная карта, флеш-память, токен и т.д.
* Свойство: биометрия (лицо, отпечаток пальца, ДНК и т.д.)

Для того, чтобы настроить 2FA на одном из учётных записей, использовано приложение Authenticator от Microsoft, и для удобства была выбрана учётная запись также из Microsoft.

Чтобы добавить запись в Authenticator, надо заново входить в учетную запись. После этого надо производить предоставление второго фактора — правильное число из данных.



Рисунок 20 — 2FA для подключения TOTP к новому аккаунту

После его прохождения станет доступным запись, при нажатии которого появляется одноразовый код, который действует в течении срока.



Рисунок 21 — Подтверждение подключение TOTP к новому аккаунту с предложением мгновенного входа без пароля.

В результате этого при попытке логина от нового устройства спрашивается подтверждение через TOTP, которого можно получать нажав на запись. Так как я не могу произвести непосредственный скриншот приложения (не разрешается из-за автоматической настройки приватности, если вам удастся, то ей Богу), внизу показан пример того, как выглядит запись с одноразовым кодом.



Рисунок 22 — Подтверждение подключение TOTP к новому аккаунту