МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ

ДЕПАРТАМЕНТ ИНФОРМАТИКИ

**Лабораторная работа № 2**

**по курсу Securitatea Sistemelor Informatice**

**Тема:**

**Управление паролями**

Выполнил: Bogdanov Iurii,

студент группы I2302

Проверила: L. Novac,

doctor conferențiar universitar

Кишинёв, 2024

***Введение:***

**Цели работы:**

1. Изучить принцип работы систем управления паролями (KeePass, LastPass,1Password, RoboForm,). Анализ их эксплуатационных параметров.

2. Сравнительное описание систем управления паролями (KeePass, LastPass, 1Password, RoboForm и т. д.)

3. Описание принципа работы системы KeePass. Изучение функциональности системы KeePass.

4. Описание принципа работы системы RoboForm. Использование RoboForm.

5. Описание принципа работы системы LastPass. Использование LastPass.

6. Описание принципа работы системы 1Password. Использование 1Password.

***Ход работы:***

Здесь мы рассмотрим каждый менеджер паролей детальнее, разберём как работает каждый, постараемся выяснить подробную информацию о каждом из них и выяснить какой же лучше и удобнее.

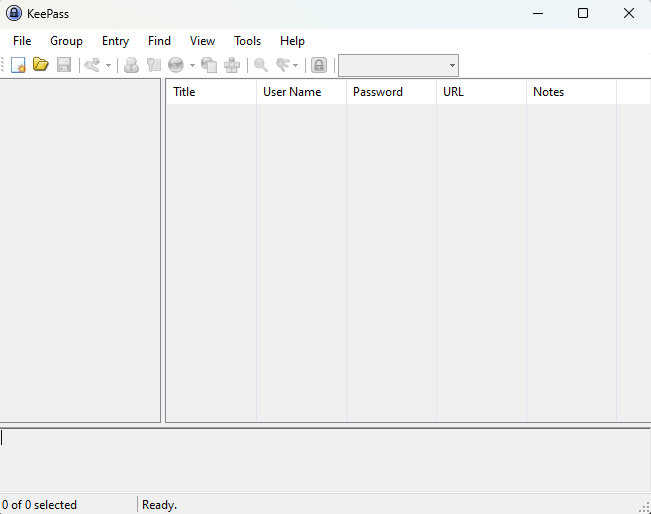
1. **Система KeePass:**

****

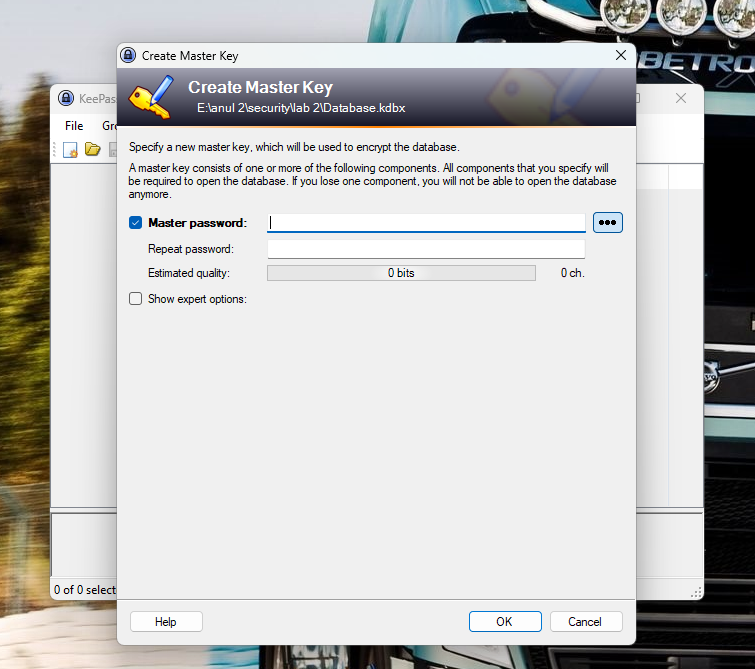
KeePass — это популярный менеджер паролей с открытым исходным кодом. Вот его основные характеристики:

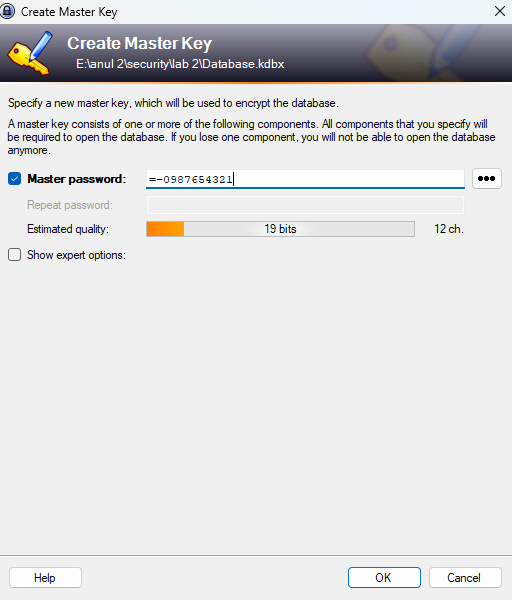
* **Открытый исходный код**: KeePass распространяется под лицензией GPL, что позволяет любому желающему просматривать и изменять исходный код.
* **Безопасное хранение данных**: Все пароли хранятся в зашифрованной базе данных с использованием алгоритмов AES-256 или ChaCha20.
* **Поддержка различных платформ**: KeePass доступен для Windows, а также существует множество портов для других операционных систем, таких как macOS, Linux, Android и iOS.
* **Мастер-пароль**: Для доступа к базе данных используется мастер-пароль, который должен быть надёжным, так как от него зависит безопасность всей базы.
* **Двухфакторная аутентификация**: KeePass поддерживает возможность использовать ключи (файлы) для дополнительной защиты наряду с мастер-паролем.
* **Плагины и расширяемость**: Благодаря поддержке плагинов можно добавлять дополнительные функции и интеграции.
* **Автозаполнение**: KeePass может автоматически заполнять логины и пароли на веб-сайтах и в приложениях.
* **Портативность**: KeePass можно использовать без установки — запускать прямо с флешки или другого внешнего носителя.
* **Офлайн-работа**: KeePass не требует подключения к интернету, что повышает безопасность.

Рассмотрим процесс работы данного менеджера паролей детальнее:



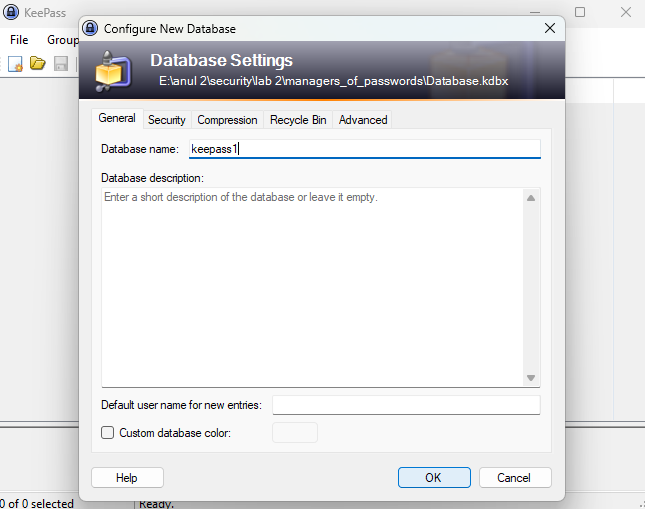
После запуска нас встречает такое окно, где можно начинать работу.Создадим первый пароль. Чтобы это сделать необходимо нажать File и выбрать Create Master Key. После этого у нас открывается данное меню.

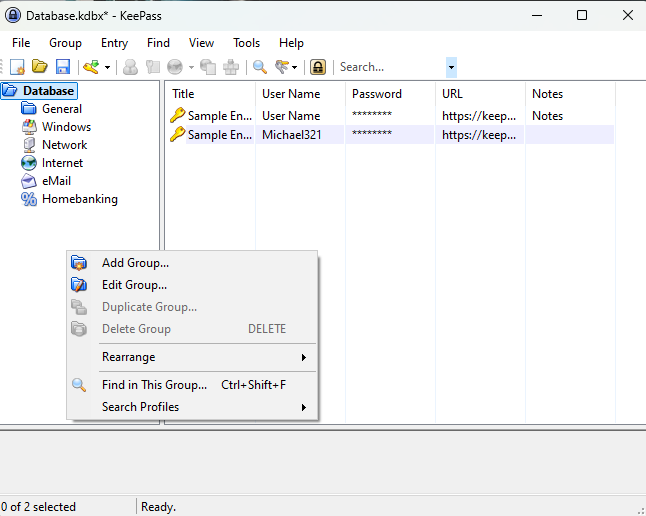




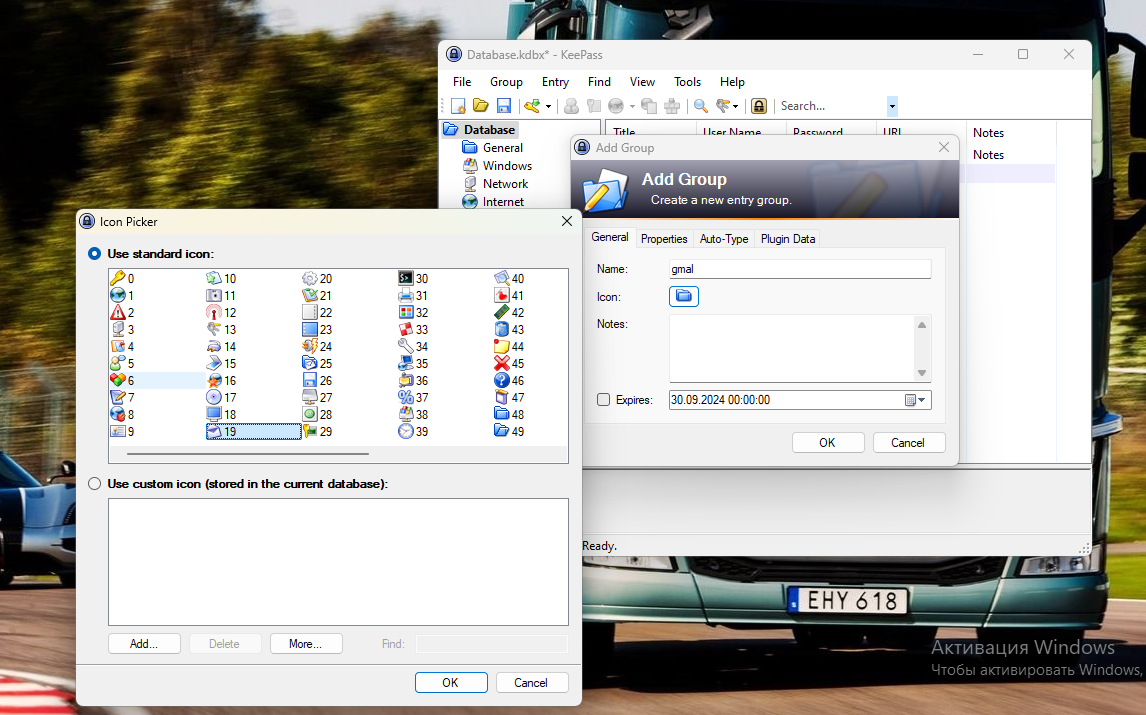
Заполняем данное поле своим паролем при этом мы видим сколько битов он занимает.

Далее мы можем попробовать создать базу данных и настроить её по своему желанию. Создать её можно нажав правой кнопкой мыши на пустое место с левой стороны и выбрать в появившемся меню Create Database.

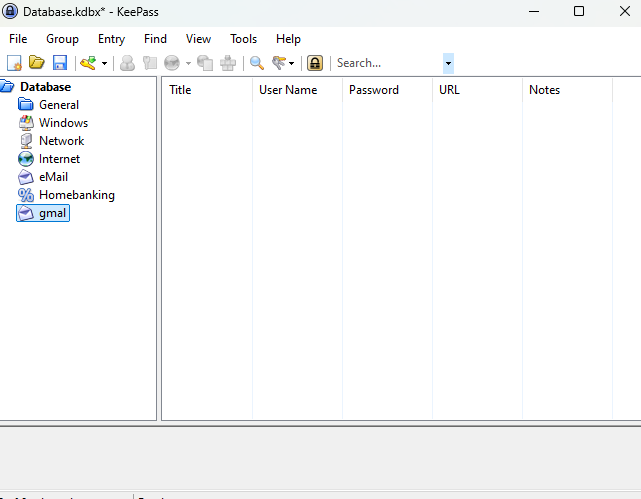




После создания базы мы можем создать группу, нажав на Database правой кнопкой мыши, выбрав при этом Add Group.

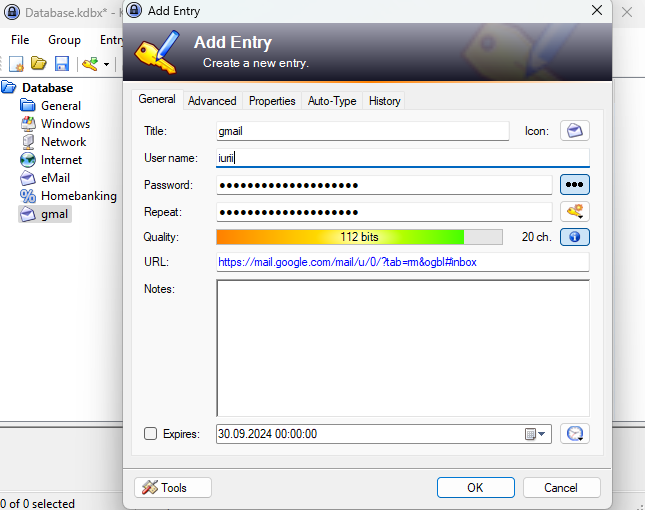


В появившемся окне мы можем настроить группу , ввести название, выбрать желаемую иконку из представленных, записать заметки если это необходимо.

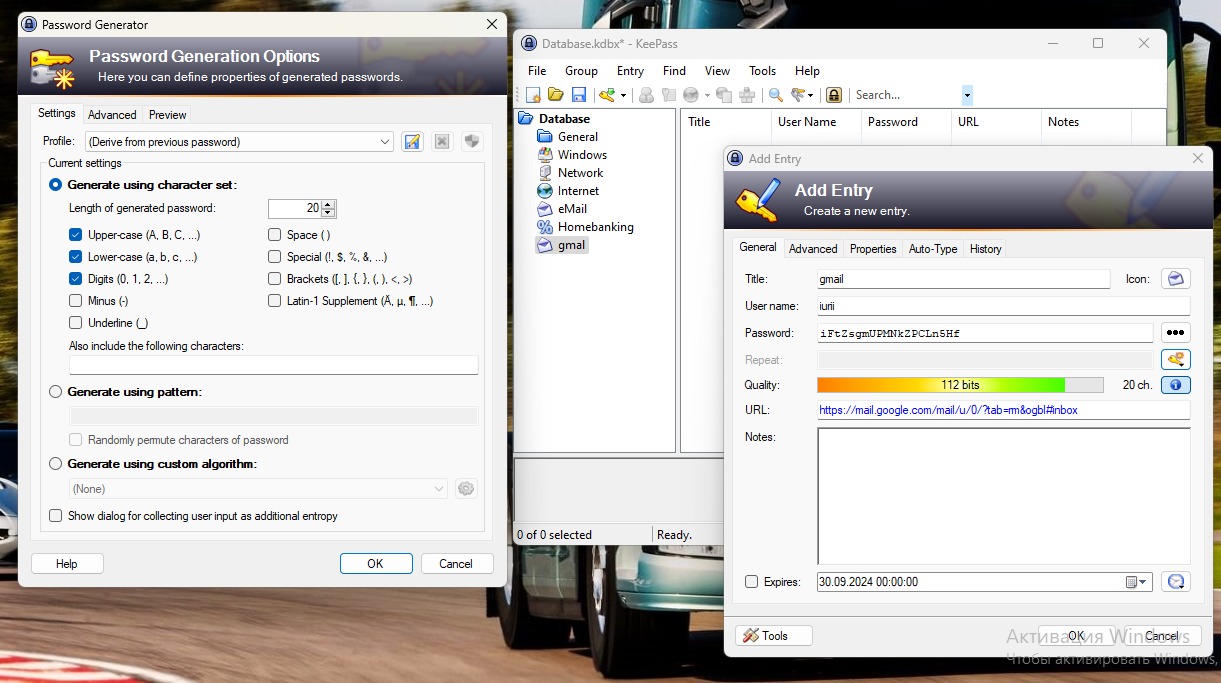


Здесь мы можем заметь, что наша группа gmail появилась в конце списка данной базы данных.

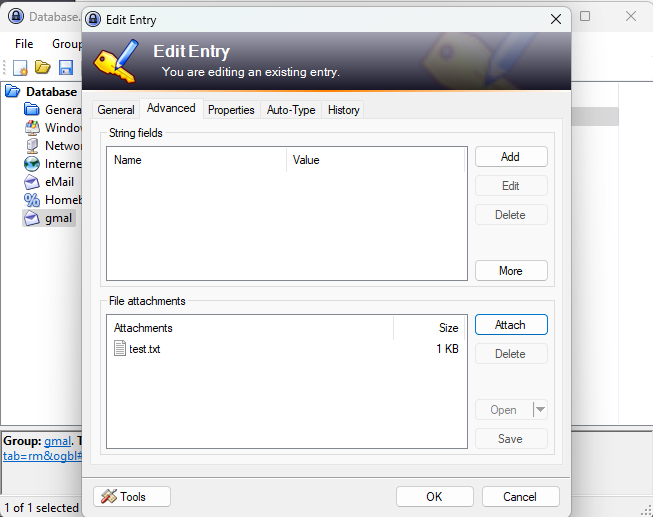
Теперь в данную группу добавим свою новую запись. Здесь также необходимо ввести название, имя пользователя, пароль и заметки если это необходимо.

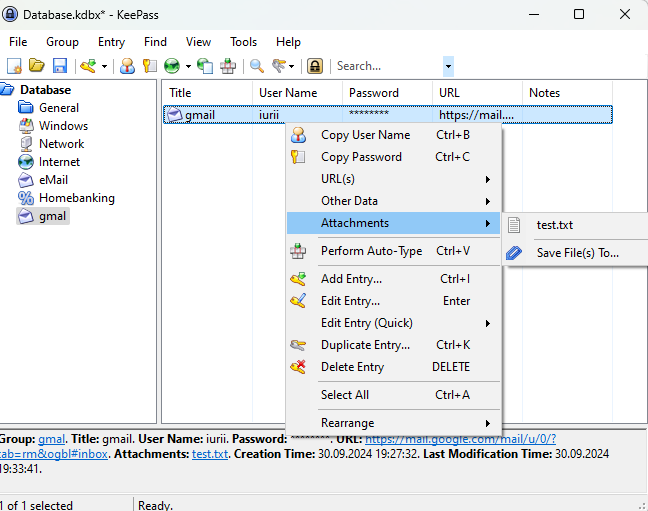


При этом мы также можем кастомизировать настройку генерации пароля нажав на три точки рядом с ним, можно выбирать длину, большие или маленькие буквы, спец. символы и другие варианты.

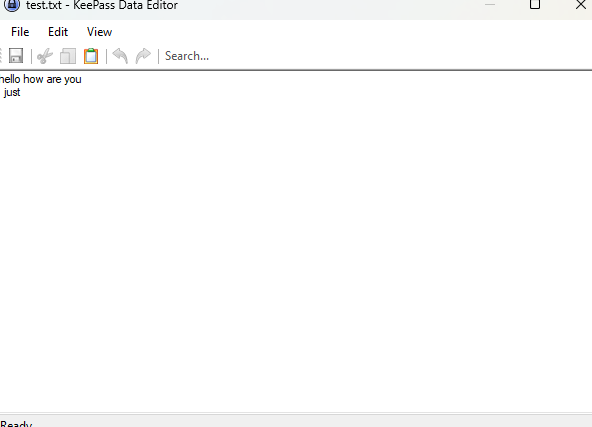


Выбрав в меню пункт Advanced открывается меню, в котром при желании мы можем прикреприть свои текстовые документы, фото или другие важные дркументы. Я это сделал на примере текстового документа test.txt нажав на Attach.

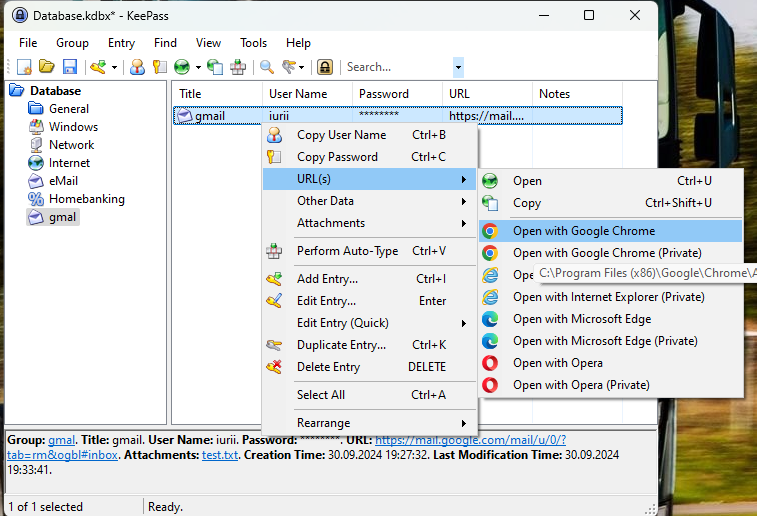




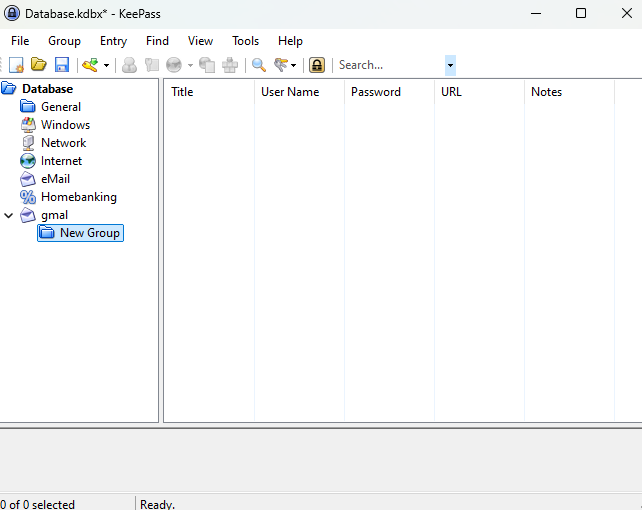
Чтобы просмотреть данный текстовый документ необходимо нажать правой клавишей мыши на нашу группу gmail, выбрать Attachments и нажать на файл. После этого он открывается и можно с ним работать.



Также здесь мы можем напрямую перейти на наш сайт, ссылку которого мы ранее записали. Это моно сделать выбрав в том же меню пункт URL (s) и перейтив любой понравившийся браузер.



Кроме этого при желании мы можем в этой группе gmail создать уже другую группу при необходимости.



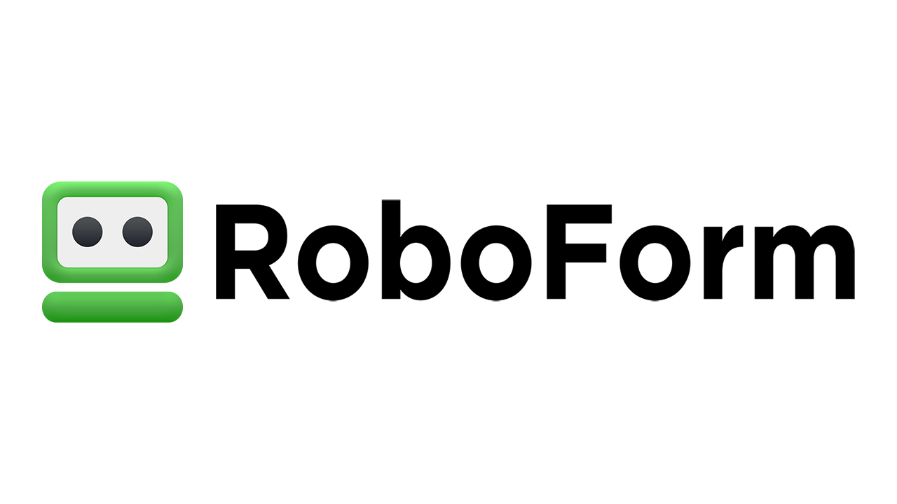
**Краткие выводы:**

### Преимущества KeePass:

* **Безопасность**: Шифрование AES-256, работает оффлайн.
* **Открытый исходный код**: Можно проверять и модифицировать.
* **Кроссплатформенность**: Поддерживает Windows, macOS, Linux, Android, iOS.
* **Расширяемость**: Поддержка плагинов для дополнительных функций.
* **Полный контроль**: База данных хранится локально, без облака.
* **Бесплатность**: Программа полностью бесплатна.

### Недостатки KeePass:

* **Сложный интерфейс**: Может показаться неудобным для новичков.
* **Нет встроенной облачной синхронизации**: Требуется ручная настройка.
* **Ограниченное автозаполнение**: Нужно устанавливать плагины.
* **Ограниченная поддержка на мобильных устройствах**: Мобильные порты могут быть неудобными.
* **Нужно делать резервные копии**: Пользователь сам отвечает за сохранность данных.

1. **Система RoboForm:**

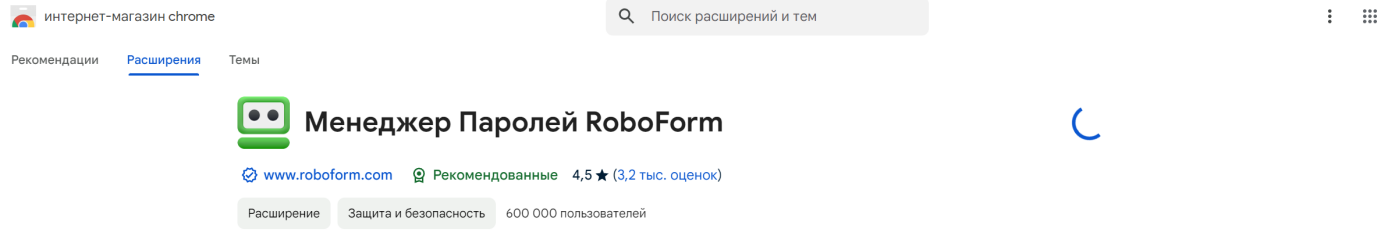
Вот краткие характеристики менеджера паролей **RoboForm**:

* **Основная функция**: RoboForm позволяет сохранять и автоматически заполнять пароли, а также управлять паролями и другой конфиденциальной информацией, такой как платежные данные, заметки и контакты.
* **Безопасность**: Использует шифрование AES-256 для защиты данных. Доступ к паролям защищён мастер-паролем, который необходимо помнить для авторизации.
* **Мультиплатформенность**: Доступен на различных платформах, включая Windows, macOS, iOS и Android. Синхронизирует данные между устройствами через облако или локально (при желании пользователя).
* **Браузерное расширение**: RoboForm интегрируется с основными браузерами (Chrome, Firefox, Edge и другими) для автоматического заполнения форм и паролей.
* **Импорт/Экспорт данных**: Поддерживает импорт паролей из других менеджеров паролей, а также экспорт паролей в текстовом виде для резервного копирования.
* **Двухфакторная аутентификация (2FA)**: Поддерживает 2FA для дополнительного уровня безопасности при входе в учетную запись.
* **Менеджер заметок**: Помимо паролей, позволяет хранить защищённые текстовые заметки.
* **Поддержка семейных и корпоративных планов**: Предоставляет семейные подписки для использования несколькими членами семьи и корпоративные решения для бизнеса.

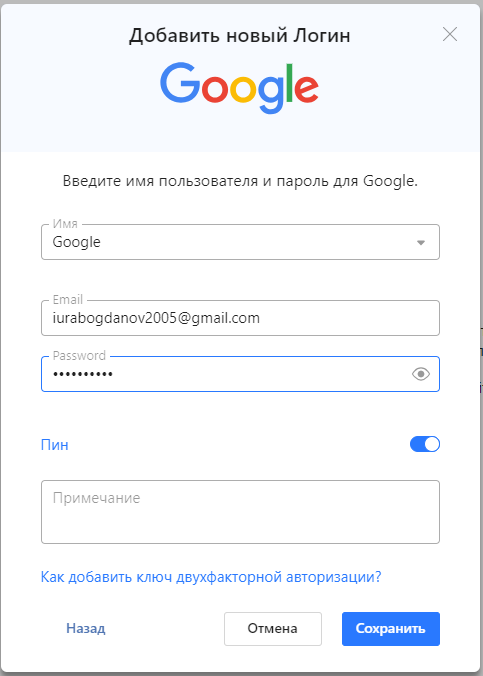
RoboForm является одним из популярных решений для безопасного управления паролями и конфиденциальной информацией.

Рассмотрим процесс работы данного менеджера паролей детальнее:

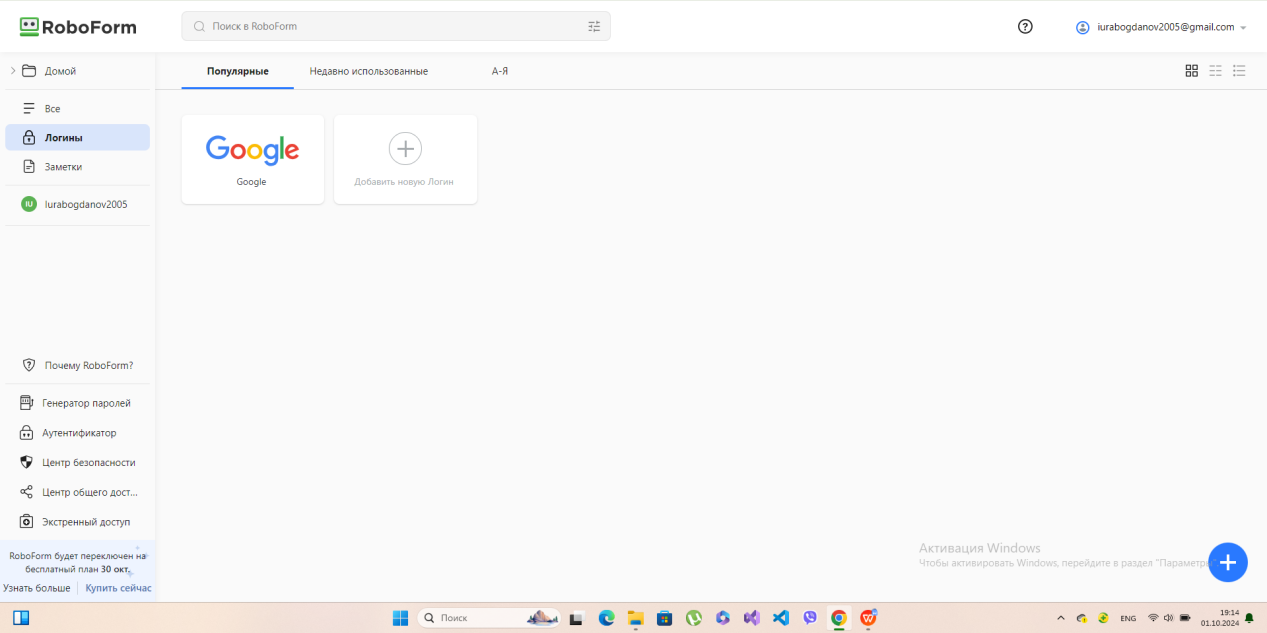
Для начала его необходимо установить в расширение браузера, а так же создать для работы свою учётную запись, что было мною сделано.



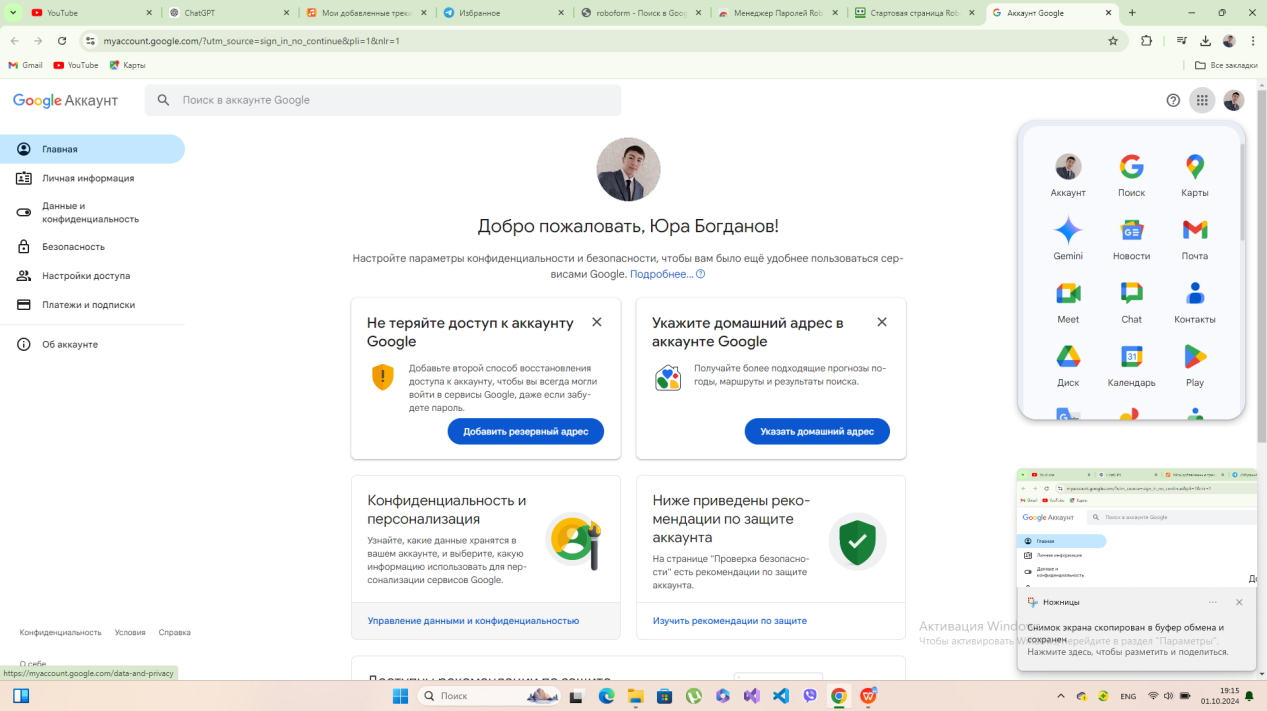
Далее я в RoboForm я добавил новый пароль для аккаунта gmail почты.

****

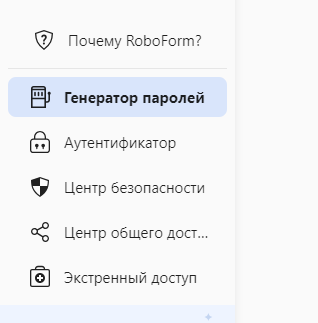
Можем заметить, что в меню менеджера, в пункте логины появился наша созданная запись.

****

Нажав на эту иконка у нас открывается гугл аккаунт в браузере.

****

Также в меню RoboForm можно выбрать дополнительные настройки такие как генератор паролей, аутентификатор, центр безопасности и другие пункты.

****

**Краткие выводы:**

### Преимущества RoboForm:

* **Удобство использования**: Простой и интуитивный интерфейс, удобен для новичков.
* **Автозаполнение**: Легко заполняет формы и логины на веб-сайтах.
* **Кроссплатформенность**: Доступен на Windows, macOS, Linux, Android, iOS.
* **Облачная синхронизация**: Автоматически синхронизирует данные между устройствами.
* **Мастер-пароль**: Один главный пароль для доступа ко всем данным.
* **Поддержка двухфакторной аутентификации**: Повышает безопасность.

### Недостатки RoboForm:

* **Платная версия**: Основные функции доступны только в платной версии.
* **Закрытый исходный код**: Пользователи не могут проверять код на уязвимости.
* **Зависимость от облака**: Для синхронизации требуется подключение к интернету.
* **Ограниченная функциональность в бесплатной версии**: Не все функции доступны бесплатно.

1. **Система LastPass:**



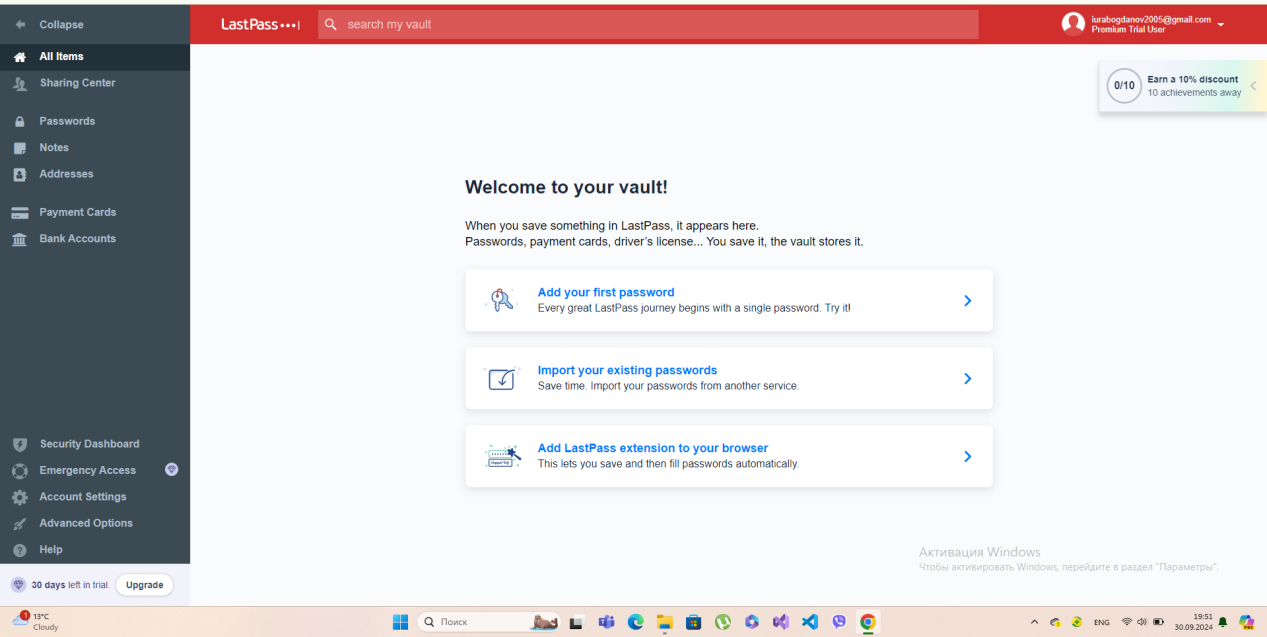
LastPass также являестя одним из популярных менеджеров паролей, который предлагает следующие ключевые характеристики:

1. **Хранение паролей**: LastPass сохраняет пароли и другую конфиденциальную информацию в зашифрованном хранилище, защищенном мастер-паролем.
2. **Кросс-платформенность**: Приложение доступно для различных операционных систем и браузеров (Windows, macOS, Linux, Android, iOS, Chrome, Firefox и др.).
3. **Автозаполнение**: LastPass автоматически заполняет пароли и данные для входа на веб-сайтах и в приложениях.
4. **Синхронизация**: Позволяет синхронизировать данные между всеми устройствами пользователя.
5. **Безопасность**: Шифрование данных происходит на устройстве пользователя (end-to-end encryption), что обеспечивает высокую степень безопасности.
6. **Генерация паролей**: Приложение предлагает встроенный генератор сложных паролей.
7. **Общий доступ**: Возможность безопасно делиться паролями с другими пользователями.
8. **Двухфакторная аутентификация (2FA)**: Поддержка различных методов двухфакторной аутентификации для дополнительной защиты.

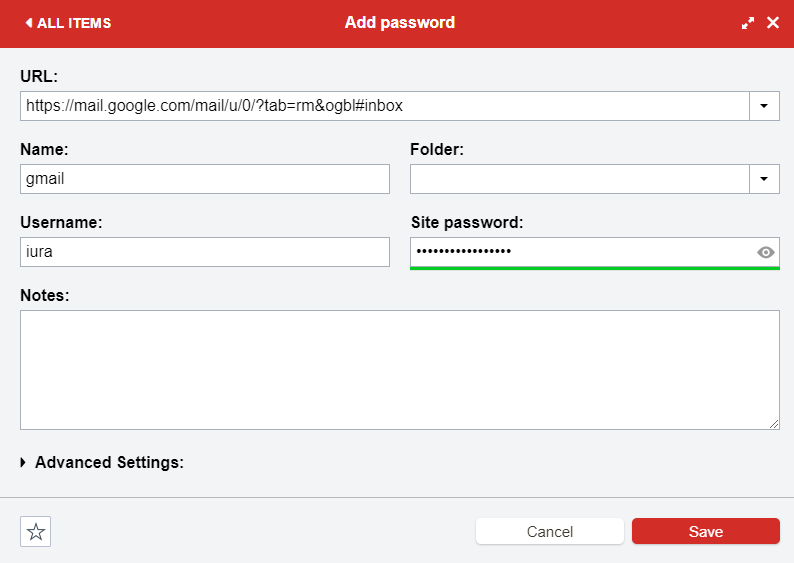
LastPass предоставляет бесплатную и премиум-версии, причем премиум-вариант включает дополнительные функции, такие как расширенные возможности безопасности и синхронизация с неограниченным количеством устройств.

Рассмотрим процесс работы данного менеджера паролей детальнее:

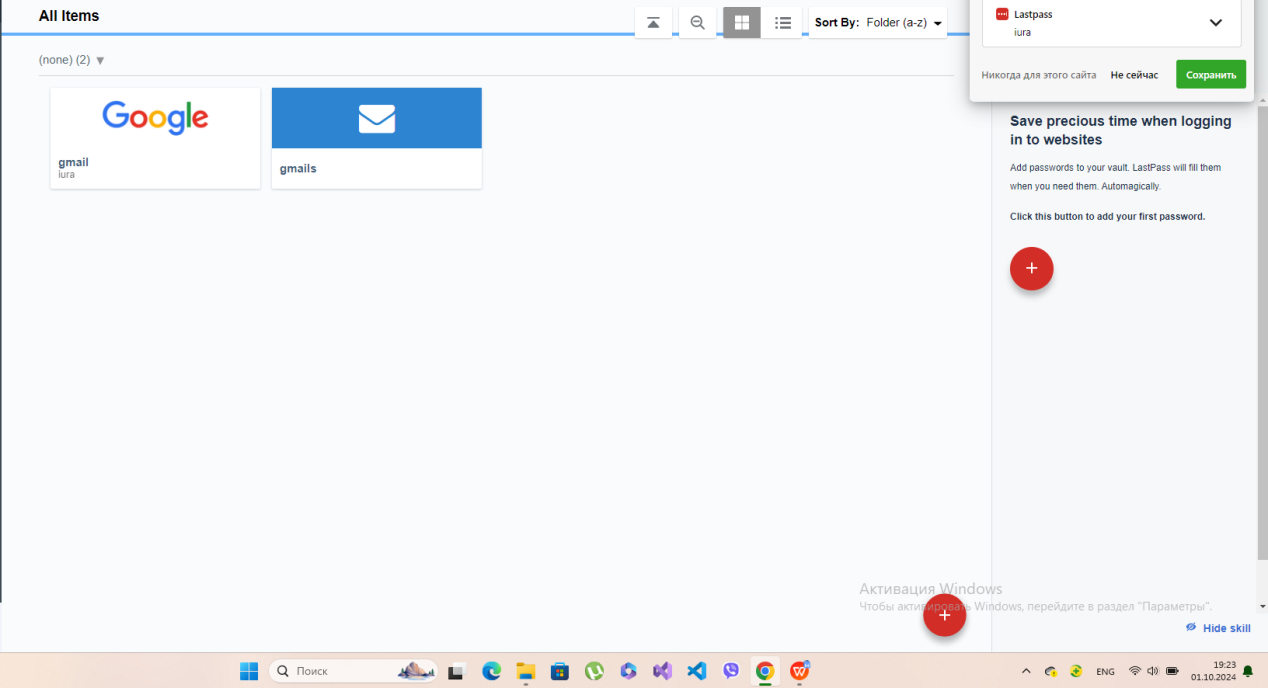
Для начала зарегистрируемся на LastPass и добавим пароль.



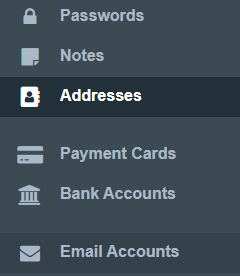
В данном окне менеджера нам необходимо выбрать пункт Add your first password , чтобы создать пароль. После этих дейсвий у нас всплывает новое окно, которое мы заполняем:



После нажатие на save мы можем заметить, что у нас появилась наша новая запись gmail в all items.



Кроме создания и записи паролей LastPass предоставляетс пользователям создавать и другие типы записей, такие как заметки, адресса, банковские аккаунты и карты, а также емайл аккаунты.



**Краткие выводы:**

### Преимущества LastPass:

* **Удобство использования**: Простой интерфейс, подходит для новичков.
* **Облачная синхронизация**: Автоматически синхронизирует пароли между устройствами.
* **Автозаполнение**: Встроенное автозаполнение для веб-форм и приложений.
* **Двухфакторная аутентификация**: Поддержка дополнительных уровней защиты.
* **Мобильные приложения**: Официальные приложения для iOS и Android с удобной синхронизацией.

### Недостатки LastPass:

* **Безопасность**: Поскольку данные хранятся в облаке, возможны уязвимости.
* **Подписка**: Бесплатная версия ограничена, для полного доступа требуется платная подписка.
* **Зависимость от облака**: Работает только при наличии интернета.
* **История утечек**: LastPass неоднократно сталкивался с проблемами утечек данных.

1. **Система 1Password:**

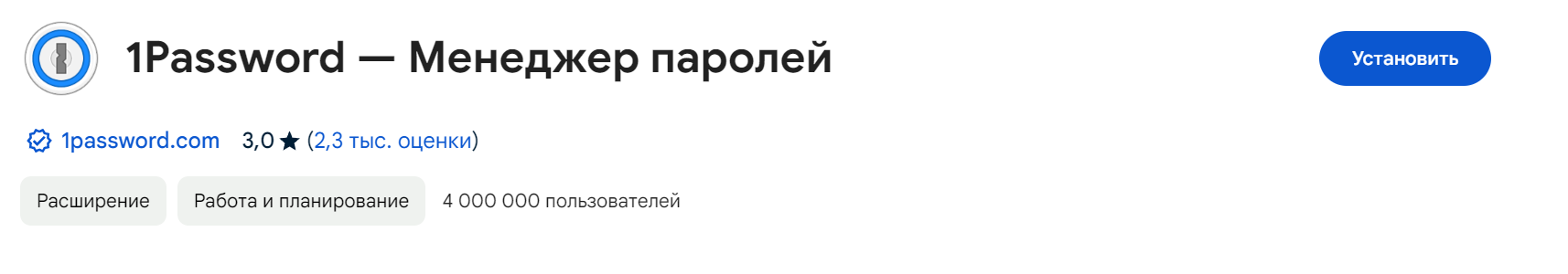


1Password — это менеджер паролей, предлагающий следующие ключевые характеристики:

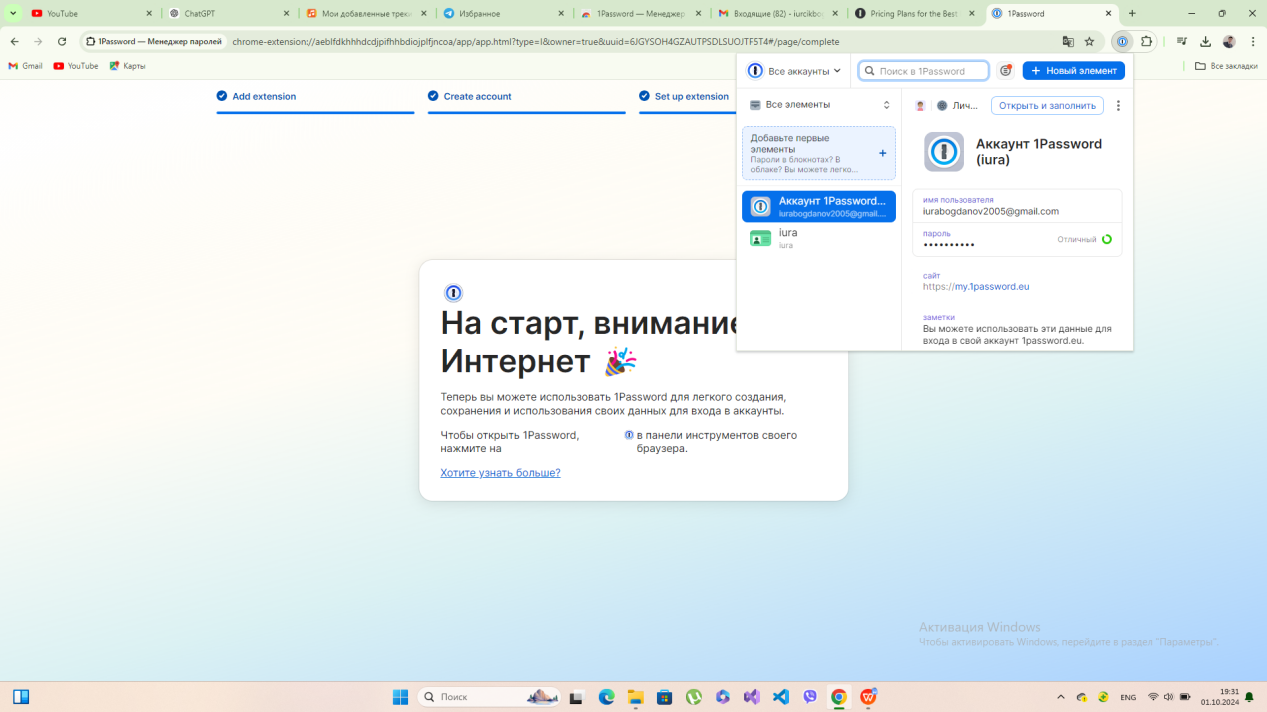
* **Безопасность данных**: Использует сквозное шифрование AES-256 для защиты данных. Пароли хранятся в зашифрованном виде и доступны только при вводе главного пароля.
* **Мастер-пароль**: Один главный пароль открывает доступ ко всем сохранённым данным. Также используется ключ безопасности, который генерируется при регистрации.
* **Кроссплатформенность**: 1Password доступен на всех популярных платформах — Windows, macOS, iOS, Android, а также через веб-интерфейс.
* **Семейные и командные планы**: Предлагаются планы для индивидуальных пользователей, семей, а также для команд и организаций с возможностью совместного использования данных.
* **Интеграции**: Поддерживает автоматическое заполнение паролей и других данных в браузерах и приложениях.
* **Менеджер паролей для приложений**: Помимо веб-сайтов, 1Password поддерживает хранение паролей для различных приложений и служб.
* **Дополнительные функции безопасности**: Включает возможности хранения другой конфиденциальной информации, например, заметок, документов, кредитных карт и другой личной информации.
* **Мультифакторная аутентификация (2FA)**: Поддержка двухфакторной аутентификации для защиты аккаунта.
* **Оповещения о взломах**: Предупреждения о возможных утечках паролей и уязвимостях для своевременного их изменения.
* **Лёгкость использования**: Удобный интерфейс с простым управлением хранилищем паролей и настройками безопасности.

### Рассмотрим процесс работы данного менеджера паролей детальнее:

Для начала его необходимо установить в расширение браузера, а так же создать для работы свою учётную запись, что было мною сделано.

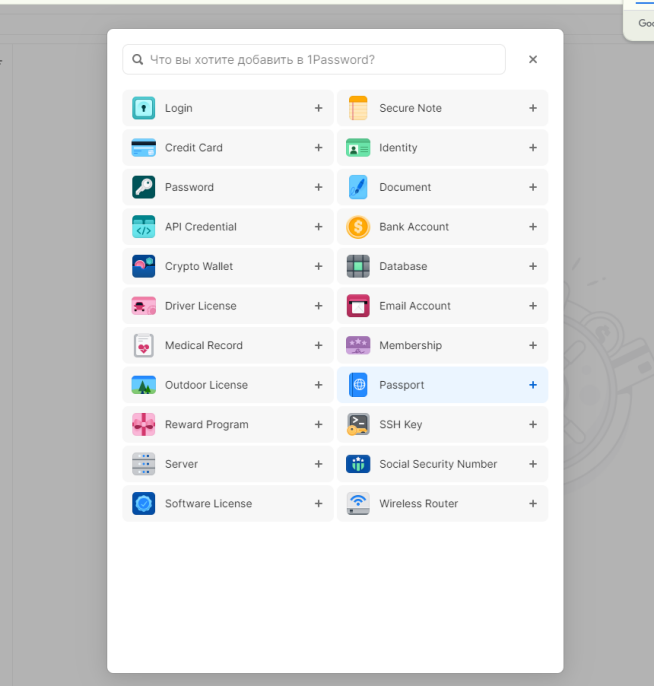
****

Выбрав в браузере данное расширение перед нами появляется данное меню, в котором мы можем начать работу, нажав на новый элемент.

****

В открывшемся окне выбираем Create one new item и из всего списка предложенного выбираем желаемый вариант.

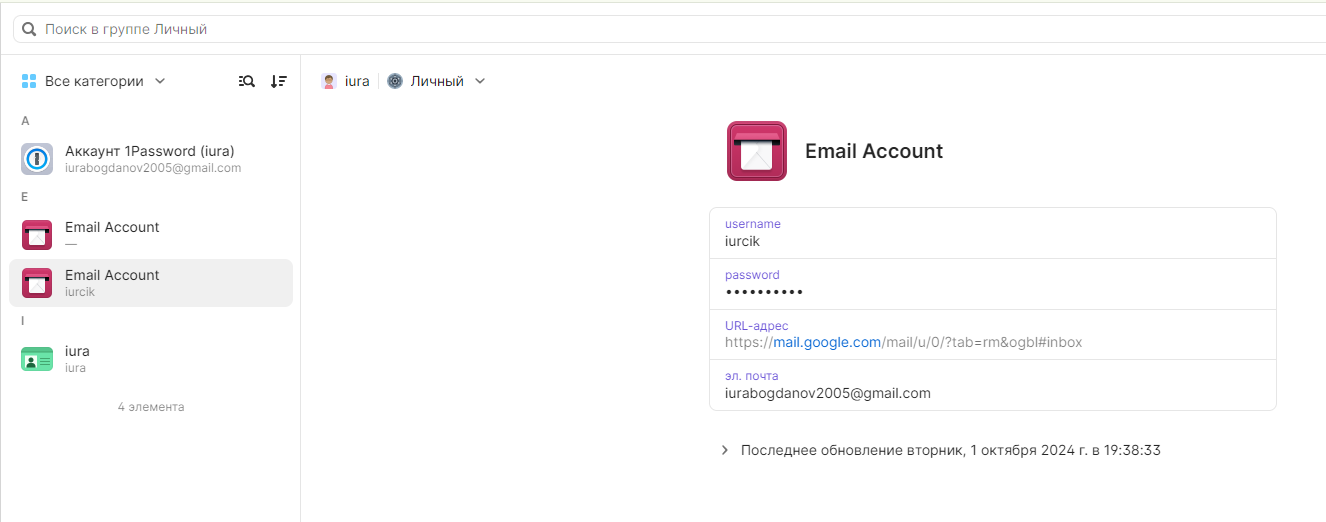
### Снимок экрана 2024-10-01 193222



В данном окне я выбрал емайл аккаунт и после этого открывается окно настройки данного пароля.

### Снимок экрана 2024-10-01 193624Снимок экрана 2024-10-01 193527В этом меню есть множество различных подпунктов, которые можно либо удалить, если в них нет нужды, либо добавить новые из списка представленных.

Теперь выбрав в основном меню пункт все элементы мы можем увидеть,что наша новая запись пароля успешно была добавлена.



### Краткие выводы:

### Преимущества 1Password:

* **Простой интерфейс**: Удобный и интуитивно понятный дизайн.
* **Облачная синхронизация**: Автоматическая синхронизация через облако между устройствами.
* **Кроссплатформенность**: Поддержка Windows, macOS, iOS, Android и веб-интерфейса.
* **Автозаполнение**: Встроенная функция автозаполнения для браузеров и приложений.
* **Двухфакторная аутентификация**: Поддержка TOTP для дополнительной безопасности.

### Недостатки 1Password:

* **Платная подписка**: Программа требует регулярной оплаты.
* **Облачное хранение**: Данные хранятся в облаке, что может быть минусом для тех, кто предпочитает локальное хранение.
* **Ограниченная кастомизация**: Меньше возможностей для настройки по сравнению с менеджерами с открытым кодом.

После проведения детального анализа каждого менаждера паролей можно составить таблицу для детального сравнения каждого мненаджера паролей, чтобы раница стала заметнее.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Критерий** | **KeePass** | **LastPass** | **RoboForm** | **1Password** |
| **1. Цена** | Бесплатно (открытый исходный код) | Бесплатный план, премиум от $3/мес | Бесплатный план, премиум от $2/мес | От $3/мес |
| **2. Кросс-платформенность** | Windows, Linux, macOS (через сторонние клиенты), iOS, Android | Windows, macOS, Linux, iOS, Android | Windows, macOS, Linux, iOS, Android | Windows, macOS, Linux, iOS, Android |
| **3. Интеграция с браузерами** | Поддерживается через плагины для Chrome, Firefox, Safari | Есть расширения для всех основных браузеров (Chrome, Firefox, Safari и т.д.) | Интеграция с Chrome, Firefox, Edge, Safari | Поддерживает все основные браузеры |
| **4. Наличие плагинов** | Да, множество сторонних плагинов | Ограниченные плагины, в основном браузерные | Поддержка дополнительных плагинов, связанных с автозаполнением и синхронизацией | Плагины доступны для интеграции с браузерами |
| **5. Дополнительные функции (генератор паролей и др.)** | Генератор паролей, настраиваемые параметры безопасности | Генератор паролей, двуфакторная аутентификация, автозаполнение | Генератор паролей, автозаполнение, поддержка 2FA | Генератор паролей, поддержка 2FA, автофокус, Travel Mode (защита данных при путешествиях) |

***Выводы по выбору лучшего менеджера паролей:***

**1Password** — самый сбалансированный вариант для **как обычных пользователей, так и для компаний**. Он предлагает высокий уровень безопасности, простой интерфейс, мультиплатформенную поддержку, и совместные функции для команд. Удобство использования, защита данных и поддержка двухфакторной аутентификации делают его привлекательным как для индивидуальных, так и для корпоративных пользователей.

**LastPass** — также хорош для **компаний и обычных пользователей**, благодаря простоте, функциональности, и возможности легко управлять доступом к паролям внутри команды. Однако, в последнее время возникают вопросы о безопасности, что может быть важным фактором для крупных компаний.

**RoboForm** — подходит больше для **индивидуальных пользователей**, особенно тех, кто ищет простой и удобный интерфейс. Однако, для компаний он менее функционален по сравнению с другими решениями.

**KeePass** — лучше всего подходит для **технически подкованных пользователей** и **компаний, которые хотят полный контроль над данными**. Однако, его сложность в использовании и отсутствие встроенной синхронизации делают его менее удобным для массового использования.

### Итог:

Для большинства пользователей и компаний **1Password** будет лучшим вариантом благодаря удобству, безопасности и широким возможностям для команд.