

МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ
ДЕПАРТАМЕНТ ИНФОРМАТИКИ

Отчет по дисциплине:
“Безопасность информационных систем”
Лабораторная работа №2
Управление паролями

Автор: Калинкова С.
группа I2302

Проверила: Новак Л.
doctor conferentiar universitar

Кишинев, 2024

Цель работы:

1. Изучить принцип работы систем управления паролями (KeePass, eWallet, LastPass, 1Password, RoboForm, Kaspersky и др.). Анализ их эксплуатационных параметров.
2. Сравнительное описание систем управления паролями (KeePass, eWallet, LastPass, 1Password, RoboForm и т. д.)
3. Описание принципа работы системы KeePass. Изучение функциональности системы KeePass. Аутентификация для разных сервисов (веб и приложений) с использованием KeePass.
4. Описание принципа работы системы RoboForm.
5. Использование RoboForm. Использование RoboForm в операционной системе iOS.

Ход работы:

1. Изучаю принцип работы систем управления паролями, прочитав несколько статей на просторах интернета с отзывами или на официальном сайте:

KeePass <https://wiki.merionet.ru/articles/keepass-что-это-и-как-пользоваться>

eWallet

<https://play.google.com/store/apps/details?id=com.iliumsoft.android.ewallet.rw&hl=ru&pli=1>

RoboForm <https://www.roboform.com/ru>

1Password

https://1password.com/personal-family-security?c=PARTNERSTK&gspk=cmljaGFyZGh1bmtlbGVyMjUxMg&gsxid=ugtZI35eok8nEY&ps_partner_key=cmljaGFyZGh1bmtlbGVyMjUxMg&ps_xid=ugtZI35eok8nEY&utm_medium=affiliate

2. Сравнительное описание систем управления паролями

Критерий	KeePass	eWallet	1Password	RoboForm
лицензии	Бесплатный (open-source)	Лицензионный (платный)	Платный (14-дневный пробный)	Платный (бесплатная версия с ограничениями)
Операционные системы	Windows, macOS, Linux, iOS, Android	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android

Совместимость с браузерами	Плагины для Chrome, Firefox, Edge	Нет браузерных расширений	Chrome, Firefox, Edge, Safari	Chrome, Firefox, Edge, Safari
Совместимость с веб-приложениями	Плагины для интеграции	Ограниченная интеграция.	Отличная совместимость	Автозаполнение форм.
Преимущества	<ul style="list-style-type: none"> - Полная бесплатность и открытый код - Высокая степень кастомизации - Поддержка множества платформ 	<ul style="list-style-type: none"> - высокая степень контроля - Простота использования и настройки 	<ul style="list-style-type: none"> - Удобный и современный интерфейс - Поддержка синхронизации между устройствами 	<ul style="list-style-type: none"> - Широкая поддержка браузеров и платформ - Удобен для корпоративного использования
Недостатки	-Ограниченные возможности для облачной синхронизации	<ul style="list-style-type: none"> - Платная версия - Ограниченные возможности для интеграции с веб-сервисами 	<ul style="list-style-type: none"> - Ограниченная бесплатная версия - Платная подписка 	<ul style="list-style-type: none"> - Ограниченная бесплатная версия - Некоторые функции требуют дополнительной оплаты
Рабочий интерфейс	- простой и функциональный	- Легкий и интуитивно понятный интерфейс	- Современный, удобный интерфейс	- Удобный интерфейс с возможностью автозаполнения
Уровень безопасности	<ul style="list-style-type: none"> - Высокая защита с помощью AES-256 - Многоуровневая защита для данных 	<ul style="list-style-type: none"> - Локальное шифрование данных - AES-256 для шифрования 	<ul style="list-style-type: none"> - AES-256 шифрование - Возможность использования двухфакторной 	<ul style="list-style-type: none"> - AES-256 шифрование - Двухфакторная аутентификация

			аутентификации	
Популярность	- Используется среди разработчиков и IT-специалистов	- Предпочитается пользователем, которым важна простота и локальное хранение данных	- Популярен среди семей и бизнес-пользователей - Широкая база пользователей	- Популярен среди корпоративных клиентов - Подходит для индивидуальных пользователей
Уникальные особенности	- Полностью оффлайн использование - Расширяемость через плагины	- Локальная синхронизация без облака	- (доступ без интернета) - Мастер-пароль и биометрия	- Автоматическая смена паролей - Корпоративные решения для управления паролями

3. Описание принципа работы системы KeePass

KeePass — это открытая и бесплатная система управления паролями, которая работает локально. Пользователь создает зашифрованную базу данных, в которой хранятся пароли, и защищает её одним мастер-паролем. Доступ к данным осуществляется через локальную программу или с помощью плагинов для интеграции с браузерами и другими сервисами. Все данные шифруются с использованием алгоритма AES-256 или ChaCha20, обеспечивая высокий уровень безопасности. KeePass может синхронизироваться с облачными хранилищами вручную, но по умолчанию не использует облачные сервисы.



KeePass
Password Safe



KeePass 2.57 released

KeePass 2.57 has been released today!

Home

You can get it here: [Download KeePass 2.57](#).

Скачиваю последнюю версию на официальном сайте

После установки запускаем программу открывается пустое окно, где можно создать новую базу данных, в которой будут храниться пароли. Это можно сделать кликнув на иконке в виде пустого листа со звёздочкой.

После этого нам предлагается установить мастер-пароль. Его нужно запомнить, так как без него доступа к базе не будет. Файл БД шифруется, так что просмотреть какой-то программой практически невозможно.

Create Master Key

C:\Users\kalin\Desktop\Database.kdbx

Specify a new master key, which will be used to encrypt the database.

A master key consists of one or more of the following components. All components that you specify will be required to open the database. If you lose one component, you will not be able to open the database anymore.

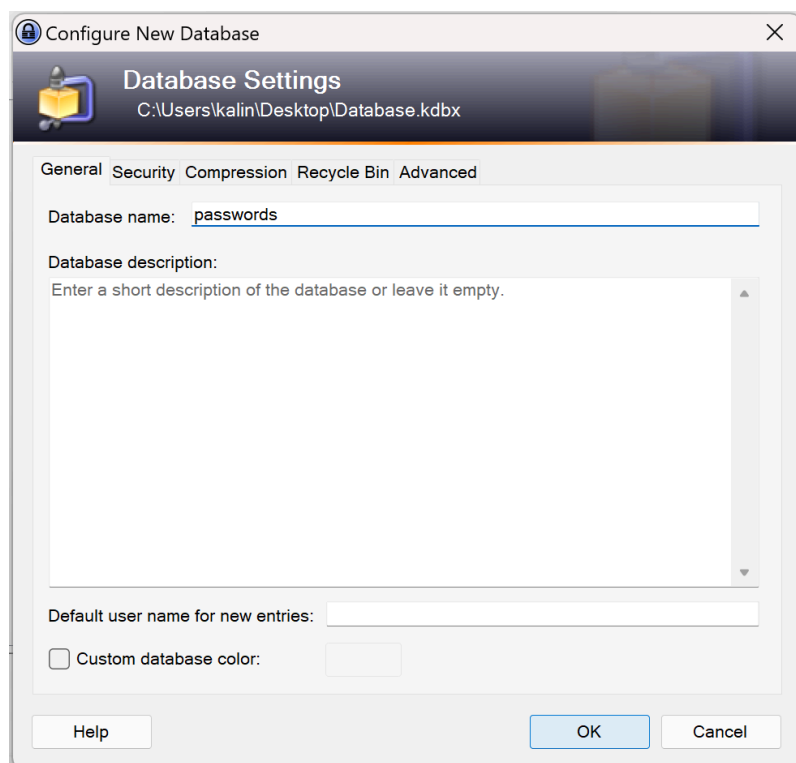
☒ Master password: [password field] [toggle icon]

Repeat password: [password field]

Estimated quality: [progress bar] 139 bits 34 ch.

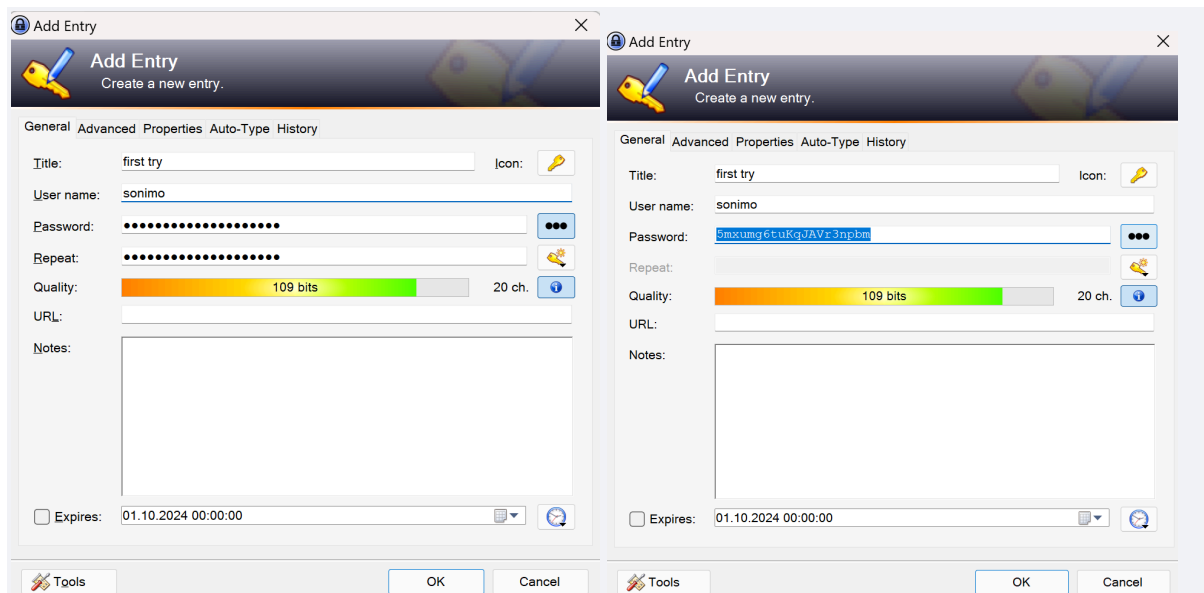
☐ Show expert options:

Help OK Cancel



И после открывается окно, где по умолчанию есть основные категории, что позволяет организованно хранить пароли. Также можно добавлять свои группы или удалять существующие. Делается это во вкладке Группа. Язык программы по умолчанию Английский.

Чтобы добавить новую запись кликаем на значке ключика с зелёной стрелкой. Также можно воспользоваться комбинацией клавиш **Ctrl + I**.



Во вкладке **general** ввожу название записи, логин и пароль. Сама программа генерирует случайный пароль, но его можно поменять. По мере ввода пароля, программа указывает его надёжность. Программа имеет встроенный генератор паролей, который можно вызвать кликнув на ключик рядом со строкой повтор пароля.

Пароль также можно просмотреть кликнув на кнопочку с тремя точками.

Add Entry
Create a new entry.

General Advanced Properties Auto-Type History

Title: first try Icon:

User name: sonimo

Password:

Repeat:

Quality: 109 bits 20 ch.

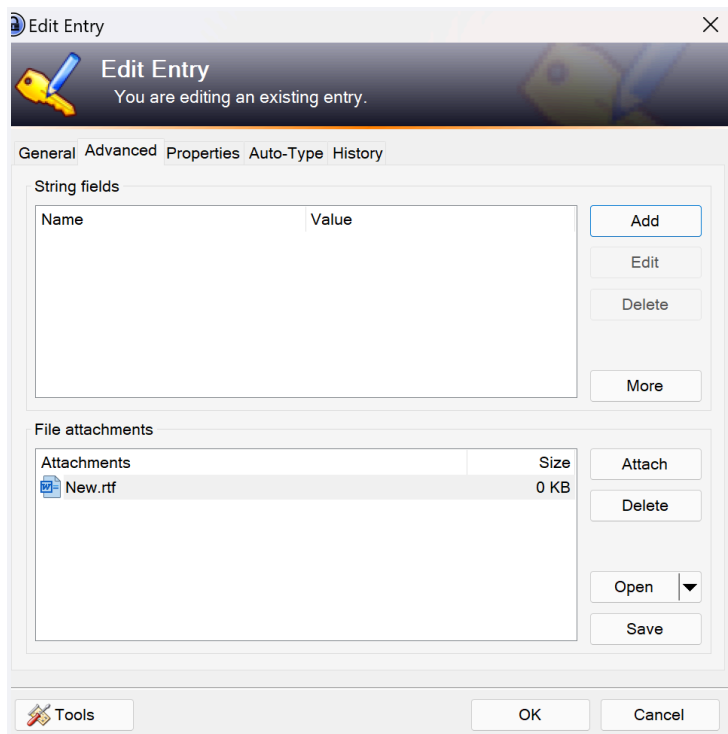
URL: <https://www.ilovepdf.com/ru>

Notes:

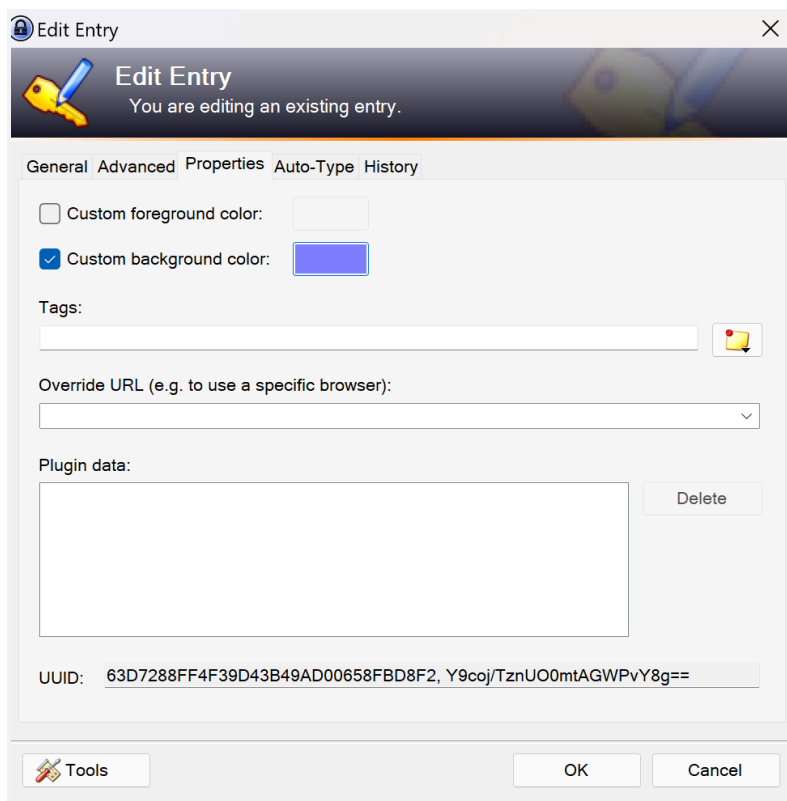
☐ Expires: 01.10.2024 00:00:00

Tools OK Cancel

Следующая вкладка **Дополнительно**. Здесь можно задать дополнительные поля или указать прикрепляемые файлы. Дополнительные поля полезны, когда вам нужно вводить, например, номер телефона, резервный электронный адрес, номер кредитки. Для этого кликаем на записи правой кнопкой и выбираем *Копировать дополнительные поля*.

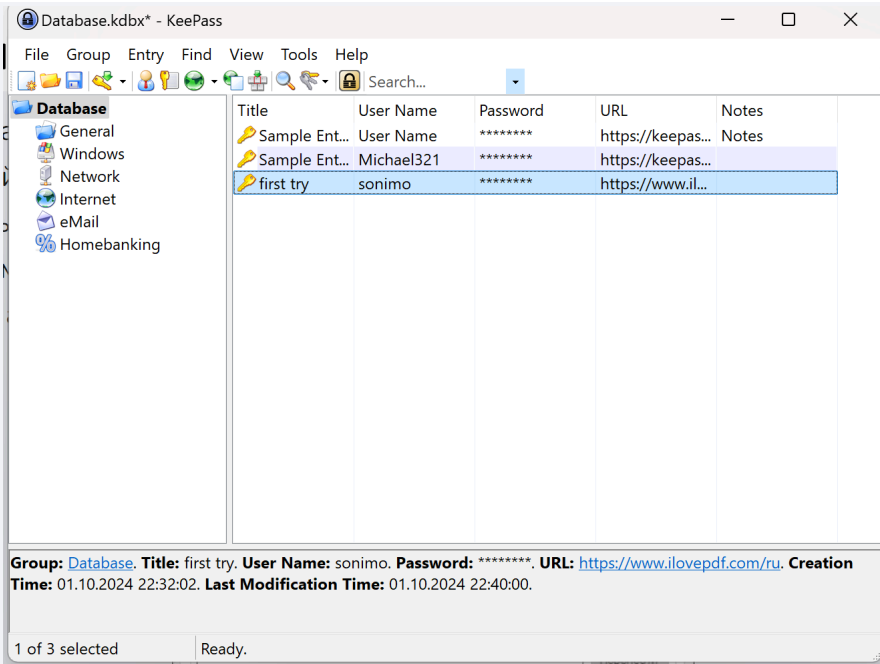


Следующая вкладка Свойства. Тут можно задать свой цвет фона для записи
полезно если вам нужно выделить конкретную запись среди сотни паролей. А
также можно переопределить используемый по умолчанию браузер.

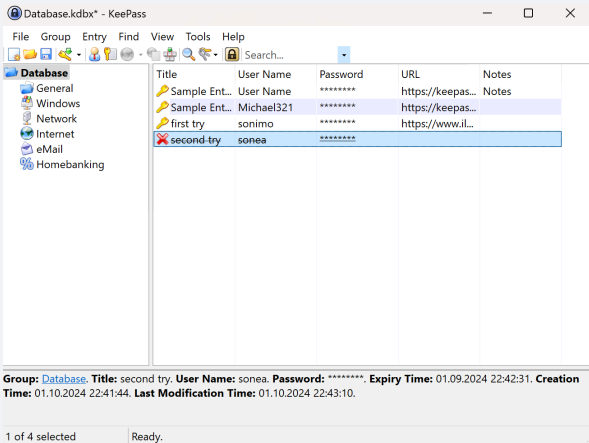
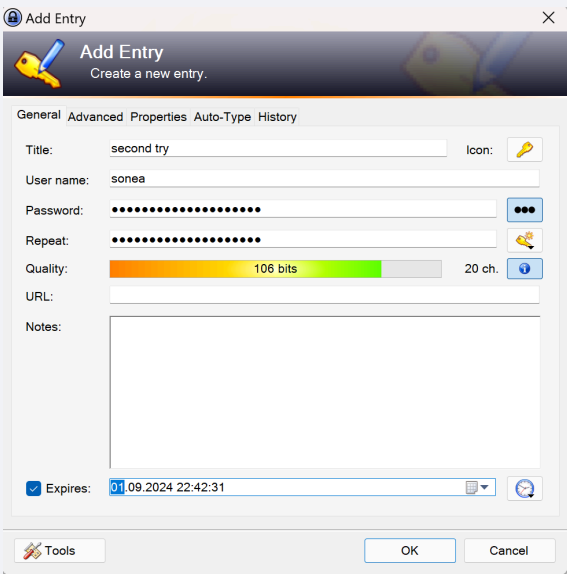


Самая, пожалуй, полезная вкладка из перечисленных это **Автонабор**.

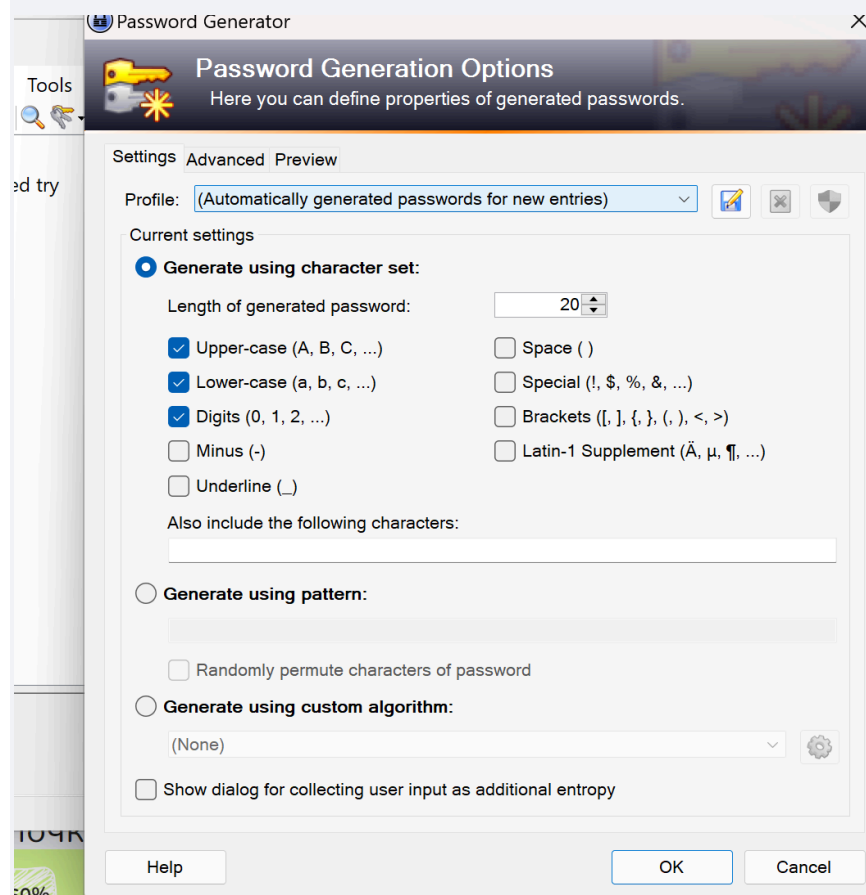
во вкладке История можно просмотреть историю изменений и при необходимости (например, поменяли пароль, но не смогли скопировать старый, чтобы ввести для смены пароля на страницы сайта) даже откатить назад.



Можно также поставить время истечения пароля. При истечении срока пароля программа выделит их красным цветом и зачёркнутым шрифтом.



Программа имеет встроенный генератор паролей, который можно вызвать кликнув на Tools -> password generator.



Выбираем какие символы хотим в пароле галочкой и программа сгенерирует список паролей, которые можно просмотреть на вкладке Просмотр.

3. RoboForm

RoboForm — это менеджер паролей и автозаполнения форм, который помогает безопасно сохранять и управлять паролями. Он автоматически заполняет логины на сайтах, генерирует сложные пароли и синхронизирует данные между устройствами. RoboForm также поддерживает функции шифрования, защищая данные пользователя.

Устанавливаю расширение для браузера



интернет-магазин chrome



Поиск расширений и те

Рекомендации

Расширения

Темы



Менеджер Паролей RoboForm



www.roboform.com



Рекомендованные

4,5 ★

(3,2 тыс. оценок)

Расширение

Защита и безопасность

600 000 пользователей

Регистрируюсь в RoboForm:



Добро пожаловать в RoboForm

Электронная почта

kalinkovasonea@gmail.com

Главный Пароль

.....



Подтвердите пароль

.....

Имя и Фамилия

sonimo

Регистрируюсь, я соглашаюсь с [Условия использования](#)
& [Конфиденциальность](#)

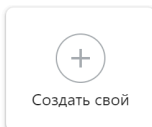
Запомните свой пароль!

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

Добавить новый Логин



Вебсайт или приложение



Создать свой

Google

Google

amazon

Amazon

PayPal

PayPal Personal

facebook

Facebook

Microsoft

Microsoft

CHASE

Chase



Apple ID

AMERICAN
EXPRESS

American Express

COSTCO
WHOLESALE

Costco Wholesale

ebay

Ebay


Capital One

Capital One

[Узнать больше](#)

Добавить новый Логин

×



Введите имя пользователя и пароль для Google.

Имя

Google

▼

Email

kalinkovasonea@gmail.com

Password

.....

👁

Пин

🔴🔵

+

Добавить примечание

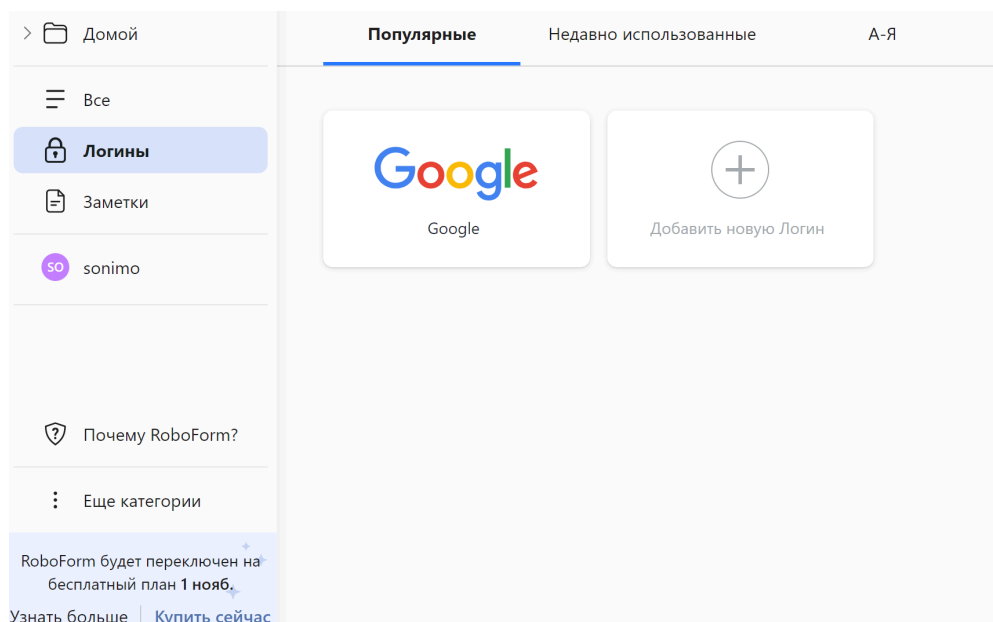
[Как добавить ключ двухфакторной авторизации?](#)

Назад

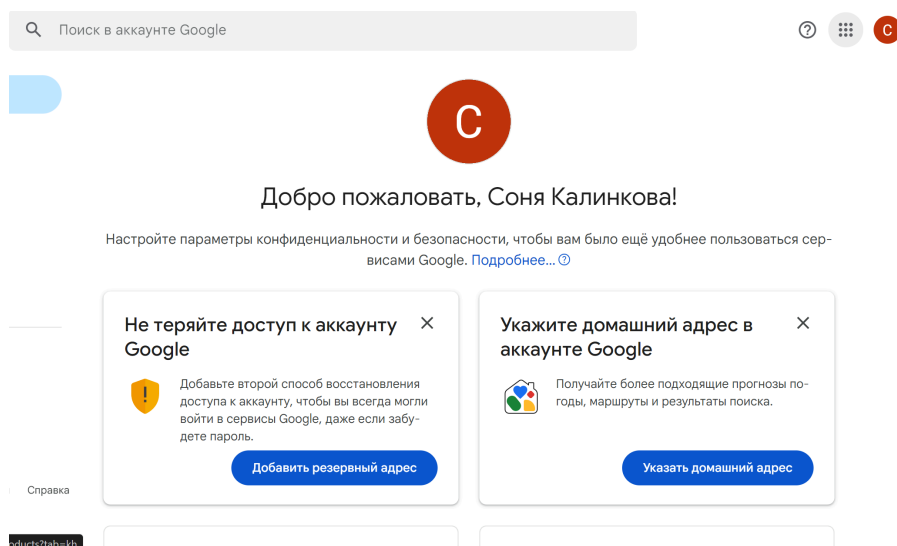
Отмена

Сохранить

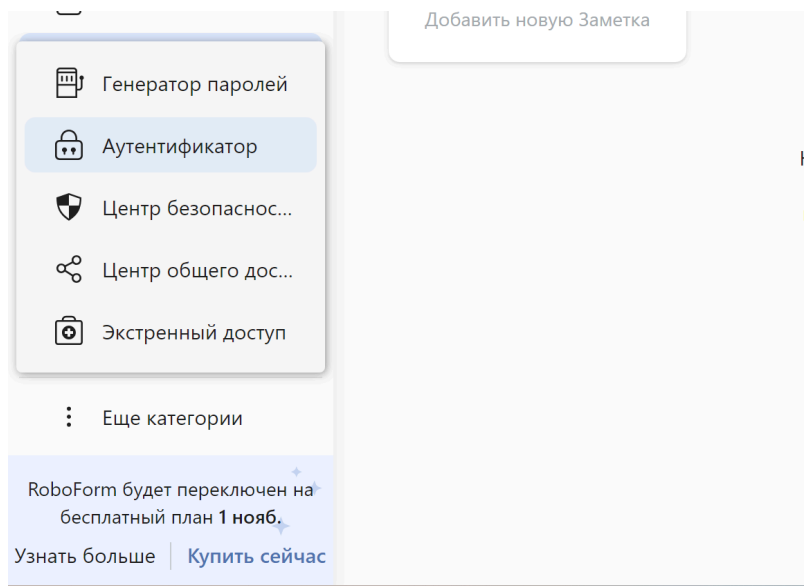
Можем заметить, что в меню менеджера, в пункте логины появился наша созданная запись.



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.



Принцип работы RoboForm:

RoboForm — это менеджер паролей и инструмент автозаполнения. Он безопасно хранит логины и пароли, предлагает сохранить учетные данные при первом вводе и автоматически заполняет их при повторном посещении сайта. Использует шифрование AES-256 и имеет генератор надежных паролей. Данные синхронизируются через облако на всех устройствах.

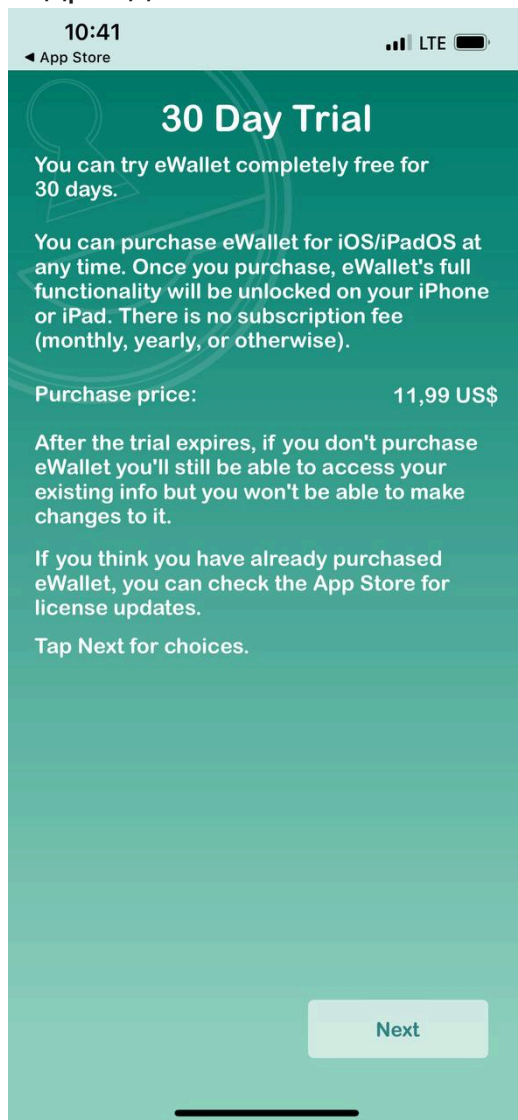
Использование RoboForm:

- **Сохранение паролей:** Автоматически сохраняет пароли.
- **Автозаполнение:** Заполняет формы регистрации и логины.
- **Генерация паролей:** Создает сложные пароли.
- **Синхронизация:** Данные доступны на компьютерах и мобильных устройствах.


Использование RoboForm в iOS:

На iOS RoboForm работает через мобильное приложение с поддержкой автозаполнения. Пользователь может загружать его из App Store, настраивать для работы с браузерами и автоматически заполнять пароли и данные на сайтах.

приложение **eWallet** платное как для iOS, windows так и для андроид





1Password

 интернет-магазин chrome

Поиск расширений и тем

Рекомендации Расширения Темы

 **1Password — Менеджер паролей**


 1password.com 3,0 ★ (2,3 тыс. оценки)


Расширение

Работа и планирование

4 000 000 пользователей

All Plans

 Business

**Individual**
Take control of your online security.

\$2.99

USD
per month. Paid annually.

Try FREE for 14 days


→

- Password generator
- Login autofill and shar
- Use on all of your devi
- Watchtower security I
- Friendly, 24/7 support

Создайте аккаунт

Имя


Sonea



Адрес эл. почты

kalinkovasonea@gmail.com


PartnerStack Referral




☐ Получайте от 1Password эл. письма с советами и информацией о последних объявлениях, новых функциях, исследовательских возможностях и событиях. Вы сможете [отписаться](#) в любое время.


Дальше


Продолжая, вы соглашаетесь с [Условиями оказания услуг](#) и [Уведомлением о порядке использования личной информации](#).

 Сохранить в RoboForm?

[Сообщить о проблеме](#)

 1password



 Информация для учетной записи будет сохранена в новый Логин '1password'

Никогда для этого сайта


Не сейчас


Сохранить

поэтому никогда не делитесь им.

Создайте резервную копию Secret Key, чтобы избежать блокировки аккаунта

A3-LL6GZX
.....

 Сохранить PDF

 Мы не храним ваш Secret Key и не можем его восстановить. Убедитесь, что вы всегда можете найти его.



1Password Emergency Kit

Created for Sonea on 02.10.2024.

If you get locked out of your account, you'll need these account details to sign in — including your **Secret Key**, which we cannot access or recover for you.

1. Get your Emergency Kit off your computer and print out a copy.
2. Fill in your account password below so you don't forget it.
3. Store it somewhere safe (such as with your birth certificate, your will, or on your personal cloud storage).

1Password Account Details

SIGN-IN ADDRESS

<https://my.1password.com>

EMAIL ADDRESS

kalinkovasonea@gmail.com

SECRET KEY

A3-LL6GZX-JCN2D4-P5EDZ-TKDSY-MQ9T3-GLW83



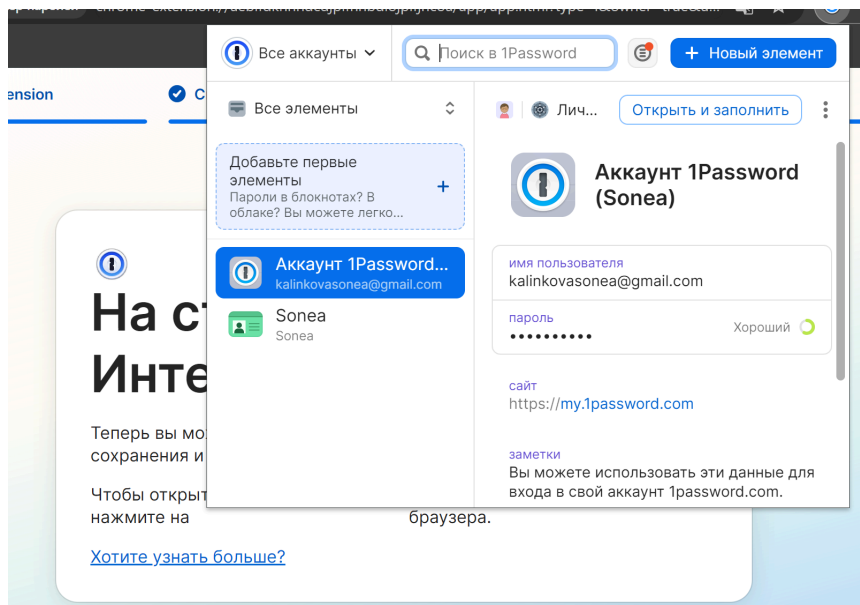
PASSWORD

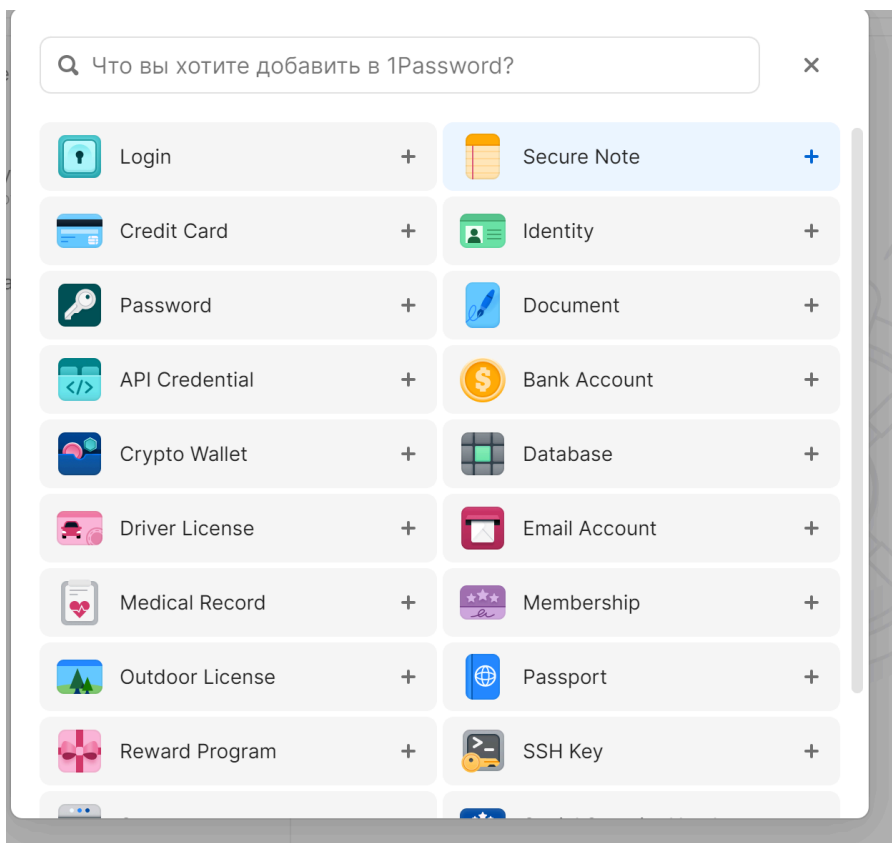
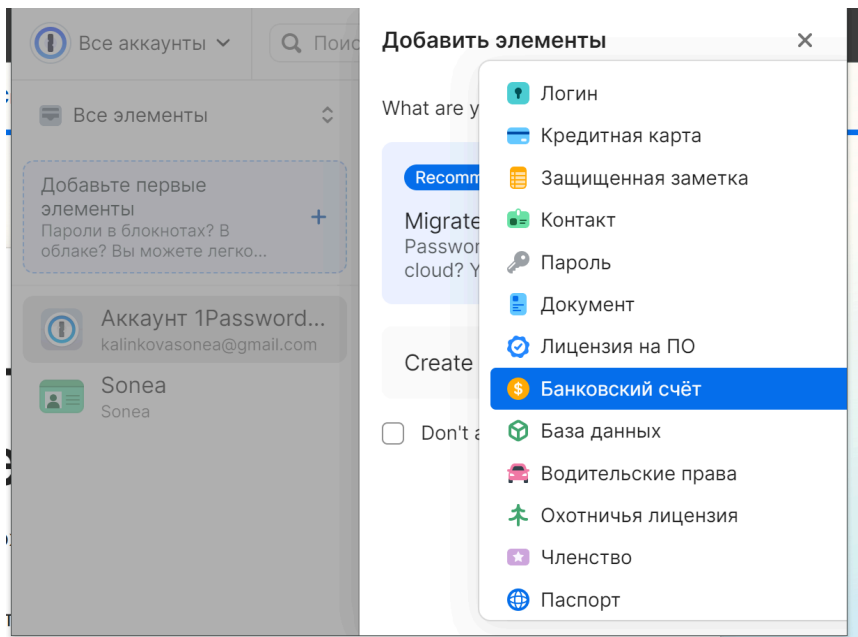


Need help?



Setup Code





←Новый элемент×

type
type

username
Sofia

server
текст

port number
текст

password
.....

security
security

auth method
auth method

URL-адрес
https://mail.google.com

ЛичныйСохранить

Поиск в группе Личный

Все категории

A

Аккаунт 1Password (Sonea)
kalinkovasonea@gmail.com

E

Email Account
Sofia

S

Sonea
Sonea

3 элемента

SoneaЛичный

ПоделитьсяРе

Email Account

username
Sofia

password
.....

URL-адрес
https://mail.google.com

эл. почта
kalinkovasonea@gmail.com

Последнее обновление среда, 2 октября 2024 г. в 10:56:44

Принцип работы системы 1Password:

1Password — это менеджер паролей, который позволяет безопасно сохранять пароли, личную информацию и другие данные. Принцип работы системы основан на шифровании данных (AES-256) и использовании "главного пароля", который защищает доступ ко всем остальным данным. 1Password автоматически запоминает логины и пароли, заполняет формы на веб-сайтах и может генерировать сложные, уникальные пароли. Данные пользователя хранятся в зашифрованном виде и могут синхронизироваться через облако на всех устройствах.

Выводы:

На мой взгляд, **KeePass** — лучший вариант среди мною рассмотренных, благодаря его финансовой доступности (бесплатному использованию). Кроме того, его возможность работать полностью офлайн обеспечивает максимальный контроль над данными.