ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ МОЛДОВЫ

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ

ДЕПАРТАМЕНТ ИНФОРМАТИКИ

**Лабораторная работа № 2**

по курсу “Securitatea Sistemelor Informatice”

Тема: Управление паролями

Проверила: Novac L. Dr. Conf. univ.   
Выполнил:Mamaliga Artur gr I2302,

Лабораторная работа №2

# Тема: Управление паролями

# Цель работы

1. Изучить работу систем управления паролями (KeePass, eWallet, LastPass, 1Password, RoboForm, Kaspersky и др.). Провести анализ их эксплуатационных параметров.

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

3. Изучить функционал системы KeePass и процесс аутентификации для различных сервисов (веб и приложений).

4. Описание работы системы RoboForm. Изучение использования RoboForm в операционной системе iOS.

# Оборудование и программное обеспечение

Операционная система: Windows/Linux/macOS

KeePass 2.x

RoboForm

LastPass

1Password

Web-браузеры: Chrome, Firefox

Мобильное устройство с iOS для тестирования RoboForm

# Часть 1: KeePass

## Описание принципа работы

KeePass — это бесплатный менеджер паролей с открытым исходным кодом, который хранит зашифрованные базы данных с паролями локально на устройстве пользователя. Он использует сильные методы шифрования (AES-256, ChaCha20) для защиты паролей. KeePass поддерживает аутентификацию с использованием мастер-пароля, ключевых файлов и различных плагинов для интеграции с другими сервисами.

## Основные функции

• Хранение паролей в зашифрованных базах данных (.kdbx файлы).

• Интеграция с браузерами через плагины для автоматической аутентификации на сайтах.

• Поддержка двухфакторной аутентификации (2FA).

• Экспорт и импорт баз данных.

## Пример работы с KeePass

1. Создание новой базы данных паролей.

2. Настройка мастер-пароля для базы данных.

3. Добавление учетных записей (например, для веб-сайтов или приложений).

4. Интеграция с браузером для автоматической подстановки паролей на веб-сайтах.

# Часть 2: RoboForm

## Описание принципа работы

RoboForm — это лицензионный менеджер паролей, который предлагает как локальное, так и облачное хранение паролей. Он предоставляет возможность автоматической аутентификации, синхронизацию данных между устройствами, а также интеграцию с различными операционными системами и браузерами.

## Основные функции

• Хранение паролей в облаке с возможностью локального хранения.

• Автоматическое заполнение форм и аутентификация на веб-сайтах.

• Мобильное приложение для iOS и Android.

• Поддержка двухфакторной аутентификации (2FA).

• Генерация паролей.

## Пример работы с RoboForm на iOS

1. Установка приложения RoboForm на iPhone.

2. Вход в учетную запись и синхронизация паролей.

3. Использование функции автоматической подстановки паролей при авторизации в мобильных приложениях и на веб-сайтах.

# Часть 3: Сравнительное описание систем управления паролями

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Система управления паролями | Стоимость | Совместимость | Преимущества | Недостатки | Интерфейс | Безопасность | Популярность |
| KeePass | Бесплатное ПО | Windows, Linux, macOS, Android, iOS | Открытый исходный код, поддержка плагинов, высокая безопасность | Отсутствие облачной синхронизации по умолчанию, требует установки плагинов для браузеров | Удобный, но устаревший интерфейс | AES-256, ChaCha20, мастер-пароль | Популярен среди IT-специалистов и разработчиков |
| RoboForm | Платное (есть бесплатная версия) | Windows, macOS, iOS, Android, Chrome, Firefox | Автоматическая синхронизация, облачное хранение, удобство использования | Платные функции, зависимость от облака | Удобный графический интерфейс | AES-256, облачная синхронизация | Популярен среди обычных пользователей |
| LastPass | Платное (есть бесплатная версия) | Windows, macOS, Linux, iOS, Android, Chrome, Firefox | Облачная синхронизация, удобство использования | В прошлом были утечки данных, платные функции | Простое и понятное | AES-256, облачная синхронизация | Широко используется в бизнесе |
| 1Password | Платное | Windows, macOS, iOS, Android, Chrome, Firefox | Высокая безопасность, поддержка мультиплатформенности | Дорогое, нет бесплатной версии | Современный и интуитивный интерфейс | AES-256, двухфакторная аутентификация | Популярен среди профессионалов и корпоративных пользователей |

# Заключение

Во время выполнения лабораторной работы мы изучили и проанализировали работу различных систем управления паролями, таких как KeePass, RoboForm, LastPass и 1Password. Каждая из этих систем обладает своими особенностями, преимуществами и недостатками, и их выбор зависит от потребностей пользователя. KeePass выделяется своей безопасностью и гибкостью, благодаря открытой архитектуре, тогда как RoboForm и LastPass обеспечивают больше удобства через облачные функции и синхронизацию.