Молдавский Государственный Университет
Факультет Математики и Информатики
Департамент Информатики

Лабораторная работа №3
по курсу “Securitatea Sistemelor Informatice”

Тема: “Аутентификация на основе нескольких факторов (Многофакторная аутентификация)”

Выполнил: Slavov Constantin,
студент группы I2302
Проверила: L. Novac,
doctor conferențiar universitar

Кишинев, 2024

- Введение: Целью данной лабораторной работы является изучение принципа работы приложения ***Rohos Logon Key***, создание токена безопасности при помощи данного приложения, проверка подлинности операционной системы (в данном случае ОС “Windows”) с использованием созданного токена безопасности, а также создание одноразового пароля и сравнение нескольких систем безопасности.

- Ход работы: Для начала, я установил на свой компьютер приложение ***Rohos Logon Key***. Буду останавливаться на каждом шаге, чтобы наглядно показать все произведенные действия.

Rohos Logon Key - это решение для двухфакторной аутентификации, которое превращает любой USB-накопитель с средство безопасности компьютера и позволяет произвести безопасную авторизацию в систему без необходимости ввода пароля или PIN-кода. Также совместимо с RFID, OTP, U2F-токенами, заменяя пароль для входа в систему Windows.

Преимущества усиленной защиты компьютера:

- Вместо простых паролей используется более безопасная система входа с аппаратными ключами: это могут быть USB-устройства, одноразовые коды из Google Authenticator, FIDO U2F или RFID-карты для доступа.

- Возможно добавить двухфакторную проверку: комбинация ключа и PIN-кода либо ключа и стандартного пароля Windows.
- Применение сложного пароля для Windows, который не нужно запоминать.

- Вход в систему происходит автоматически и моментально благодаря использованию электронного ключа.

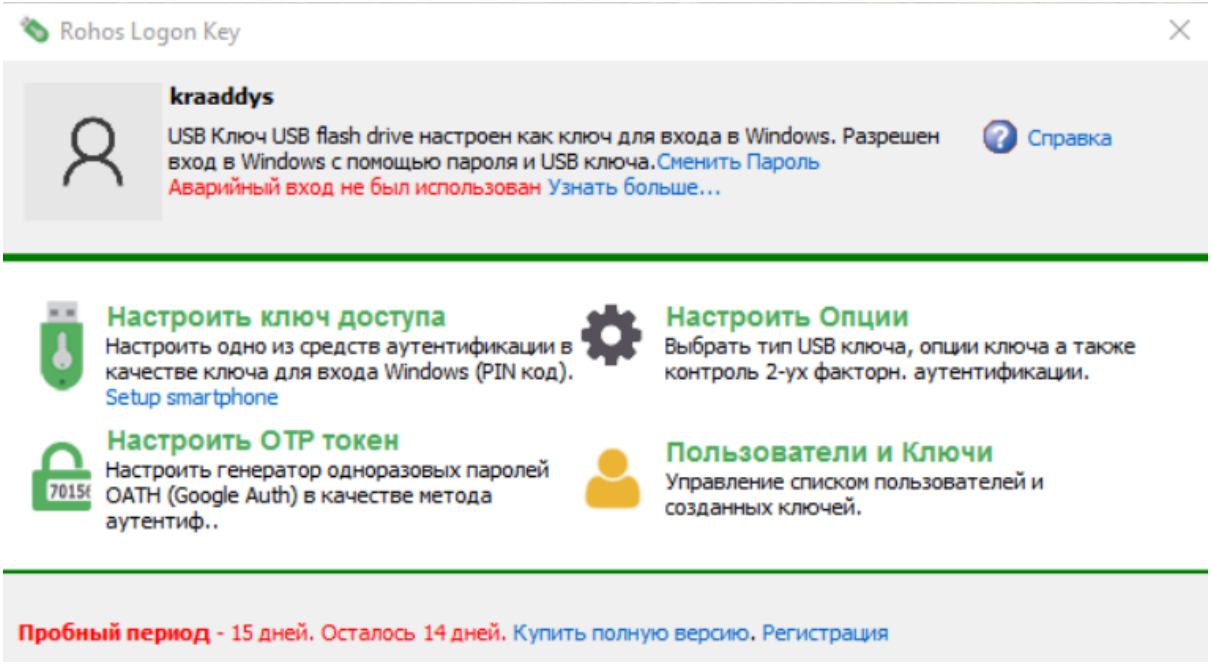
- Для подтверждения операций с повышенными правами достаточно одного клика при запросе контроля учетной записи.

- Ваш компьютер защищен паролем, но вам не нужно вводить его вручную каждый раз при входе, разблокировке или изменении настроек.

- Защита доступа сохраняется даже при входе в Windows в безопасном режиме или при удалённом подключении.

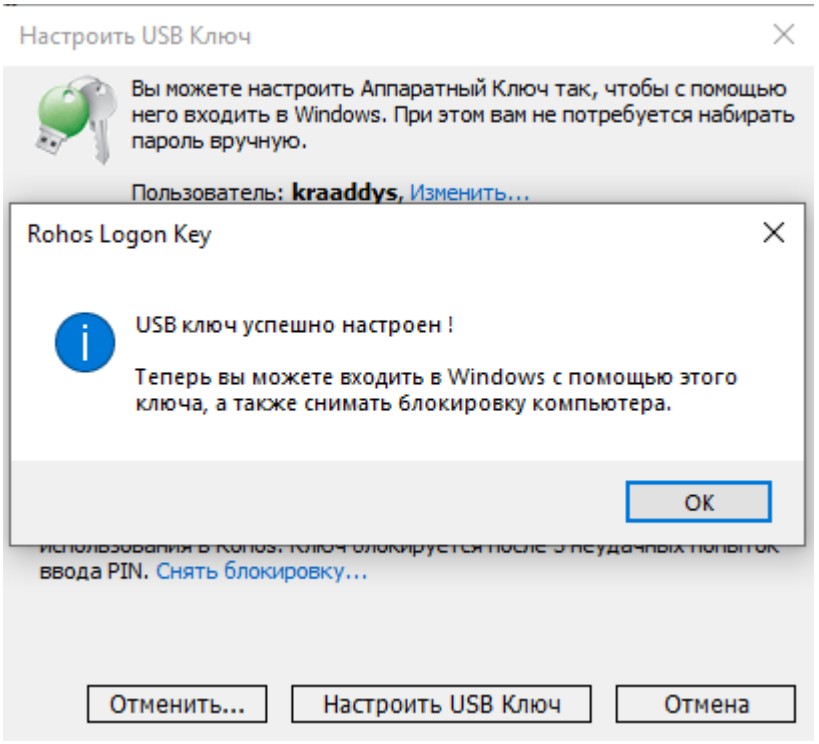
- Поддерживаются различные способы аутентификации: обычные USB-накопители, SD-карты, PKCS#11-ключи безопасности (например, SafeNet iKey, eToken, Feitian), FIDO U2F, одноразовые коды из Google Authenticator или YubiKey, смартфоны с Rohos push или Bluetooth ID, а также RFID-карты (MiFare, Desfire, EM-Marine и другие). Совместимость с Windows Hello.

- Используются проверенные методы шифрования данных от NIST (National Institute of Standards and Technology): пароли не сохраняются в открытом виде на ключе, а копирование ключей USB без разрешения невозможно. Все данные на ключе зашифрованы по стандарту AES с длиной ключа 256 бит.

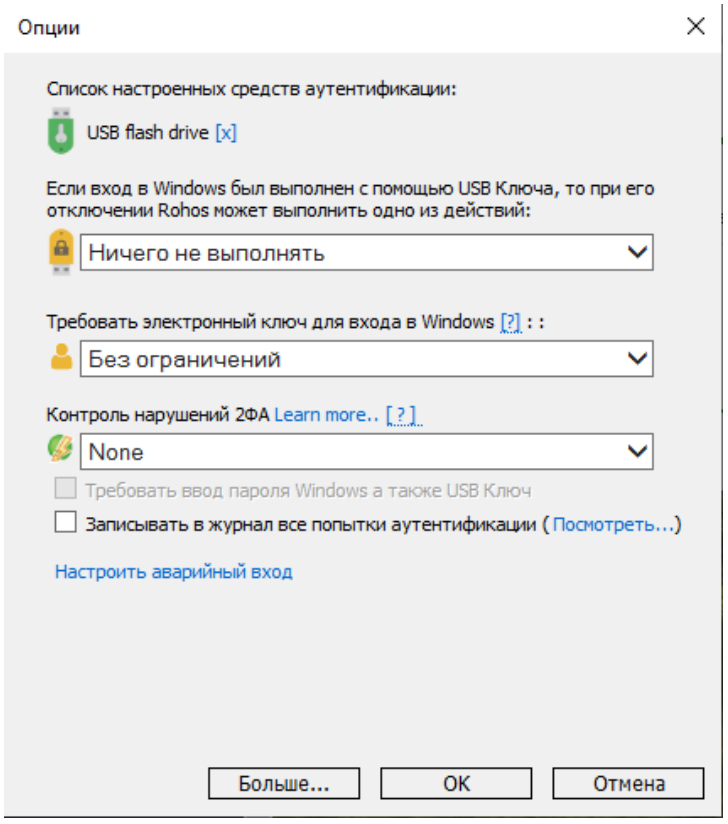


В главном меню можно выбрать из нескольких предложенных вариантов настройки ключей доступа и токенов. Мне необходимо выбрать пункт “Настроить ключ доступа” для того, чтобы настроить одно из средств аутентификации в качестве ключа для входа в Windows. В данном случае, в качестве ключа доступа мне послужит обычная USB-флешка, которую необходимо подключить к компьютеру.

Открыв меню настройки ключа, необходимо настроить несколько параметров: выбрать тип устройства или метод аутентификации, выбрать в проводнике подключенное устройство и задать ему соответствующий пароль.



Я смог ввести данные и настроить свой USB-ключ, а также испытал его в действии, чтобы убедиться, что все работает как нужно. После всех манипуляции, я смог без проблем войти в систему при помощи внешнего USB-накопителя.



Выше на скриншоте представлен список опции для настроенных средств аутентификации. Я не стал ничего изменять и оставил все по умолчанию.

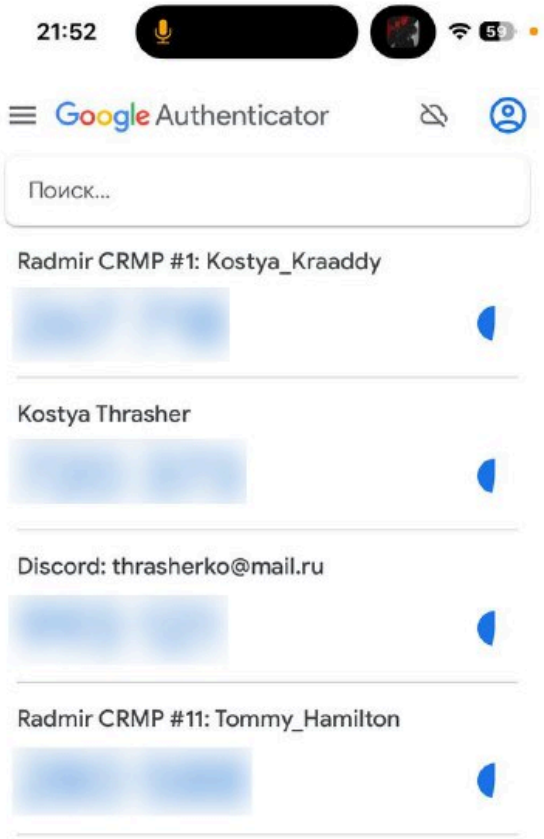
Таким образом, у меня получилось создать ключ для входа в систему при помощи внешней USB-флешки, что значительно упростило процедуру авторизации.

- Дополнительно: Google Аутентификатор в моей повседневной жизни и принцип его работы.

В качестве повседневного средства защиты данных от аккаунтов я использую Google Аутентификатор. Это очень удобное средство для генерации одноразовых паролей, каждый из которых имеет срок в 30 секунд.

Я использую данное приложение для защиты аккаунтов всех соц.сетей, которые у меня есть, игровых аккаунтов, почты и т.д.
Здесь очень удобный интерфейс и можно легко разобраться в функционале приложения.

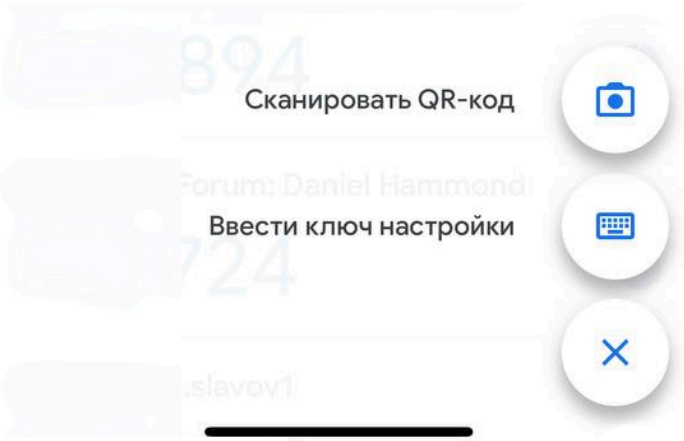
Главный экран приложения:



На главном экране приложения указаны все актуальные одноразовые пароли для входа в аккаунты. У меня их намного больше, я показал лишь часть из тех, что у меня есть.

Данные из приложения Google Аутентификатор можно легко перенести с одного устройства на другое при помощи нескольких методов:
- QR-кода
- Ключ настройки

Желательно переносить данные на запасное устройство, потому что в случае утери данных их восстановление становится невозможным.



Стоит отметить, что приложение работает оффлайн и для его работы не обязательно иметь стабильное подключение к интернету. Приложение использует несколько методов шифрования данных:
- **HMAC (Hash-based Message Authentication Code)**: Это метод шифрования, использующий секретный ключ для генерации одноразовых паролей.
- **Алгоритмы SHA-1 и SHA-256**: Google Authenticator использует хеш-функции SHA-1 (для HOTP) и SHA-256 для обеспечения безопасности.

- Вывод: Для меня приложение Google Аутентификатор стоит на первом месте в плане дополнительной защиты аккаунтов, я использую его довольно-таки большое количество времени и пока никаких сбоев или других проблем не обнаружил.

Сравнительная характеристика систем одноразовых паролей (OTP)

- RSA SecurID:
RSA SecurID — это средство для двухфакторной аутентификации, разработанное компанией RSA Security (часть Dell Technologies). Оно добавляет дополнительный уровень безопасности, требуя не только стандартный пароль, но и использование физического токена для генерации одноразовых паролей (OTP).

Основные особенности:
- RSA SecurID поддерживает как физические устройства (например, токены с экраном), так и виртуальные токены, которые могут работать на смартфонах.
- Токены создают динамические одноразовые пароли, обновляющиеся каждые 60 секунд, что существенно улучшает безопасность.
- Поддерживается интеграция через различные протоколы, такие как RADIUS, и взаимодействие с разнообразными системами.
- Встроенные функции адаптивной аутентификации, анализирующие контекст пользователя для оптимизации безопасности.
- Комбинирует использование пароля и токена для усиления защиты.

- McAfee One Time Password:
McAfee OTP является частью общего решения от McAfee и предназначено для создания одноразовых паролей с целью повышения уровня безопасности при доступе к важным ресурсам.

Ключевые черты:
- Использует программные токены, такие как мобильные приложения, для генерации одноразовых паролей.
- Интегрируется с другими продуктами McAfee, создавая целостный подход к безопасности.
- Поддерживает генерацию временных паролей, которые действуют в течение определенного промежутка времени.
- Использует стандартные методы безопасности McAfee для обеспечения дополнительной защиты, например, проверку наличия антивирусов.

Сходства и отличия RSA SecurID и McAfee OTP:
- Оба решения используют как программные, так и аппаратные токены для усиления аутентификации.
- Оба продукта могут быть интегрированы с различными системами и сервисами.
- Оба решения поддерживают многофакторную аутентификацию.
- RSA SecurID имеет более продвинутые возможности адаптивной аутентификации, тогда как у McAfee это зависит от настройки и интеграции.

- Алгоритм HOTP (RFC 4226):
HOTP (HMAC-Based One-Time Password) — это алгоритм, который генерирует одноразовые пароли с использованием технологии HMAC. Он описан в стандарте RFC 4226.

Ключевые компоненты:
- Секретный ключ: Используется для генерации HMAC и является известным и серверу, и пользователю.
- Счетчик: Обновляется после каждой успешной аутентификации. Сервер и клиент синхронизируют значения.
- Хеш-функция: Алгоритм SHA-1 (или более продвинутые, такие как SHA-256) используется для генерации OTP.
- Длина пароля: Обычно длина одноразового пароля составляет 6 цифр.

Процесс генерации:
- Генерируется HMAC на основе секретного ключа и счетчика.
- Хеш-функция преобразует результат в одноразовый пароль.

Процесс верификации:
- Сервер повторно генерирует одноразовый пароль с теми же параметрами, что и клиент.
- Если оба OTP совпадают, аутентификация успешна.

Преимущества HOTP:
- Одноразовые пароли значительно уменьшают риск компрометации.
- Простота реализации и высокая производительность.
- Использование стандартизированных криптографических методов (HMAC, SHA) делает его надежным выбором для различных приложений.

- Single Sign-On (SSO):
SSO — это метод, позволяющий пользователю войти в одну систему и получить доступ к нескольким приложениям без необходимости вводить пароль каждый раз.

- OpenID:
OpenID — это открытый протокол, который позволяет пользователям использовать единый идентификатор для входа на различные сайты, поддерживающие этот стандарт. Примеры провайдеров OpenID включают Google и Yahoo.

- Windows Live ID:
Windows Live ID, ныне известный как Microsoft Account, позволяет получить доступ к множеству сервисов Microsoft с использованием одного аккаунта. Это единая система входа, тесно интегрированная с такими продуктами, как Outlook, OneDrive и Skype.

Сходства между OpenID и Windows Live ID:
- Оба обеспечивают единый вход (SSO) для доступа к множеству сервисов.
- Оба уменьшают необходимость запоминания множества паролей.

Различия:
- OpenID — это открытый стандарт, поддерживающий разных провайдеров.
- Windows Live ID ориентирован на экосистему Microsoft.

- Вывод:

Rohos Logon Key обеспечивает двухфакторную аутентификацию с использованием USB-ключа для единого входа (SSO). **OTP** системы генерируют одноразовые пароли, которые действуют только ограниченное время, добавляя уровень защиты. HOTP, будучи разновидностью OTP, использует HMAC для создания одноразовых паролей, что делает его надежным средством аутентификации. OpenID и Windows Live ID облегчают процесс входа, минимизируя необходимость создания новых учетных записей.

Все описанные методы добавляют дополнительный уровень безопасности за счет использования многофакторной аутентификации и стандартов шифрования. Выбор подходящего метода зависит от конкретных потребностей и сценариев использования.