

МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ
ДЕПАРТАМЕНТ ИНФОРМАТИКИ

Отчет по дисциплине:
“Безопасность информационных систем”
Лабораторная работа №3
Многофакторная аутентификация

Автор: Калинкова С.
группа I2302

Проверила: Новак Л.
doctor conferentiarius universitar

Кишинев, 2024


Цель работы:

- ✓ • Создание токена безопасности с помощью Rohos Logon Key, (Rohos face Logon).
- ✓ • Проверка подлинности Windows с использованием созданного токена безопасности.
- ✓ • Одноразовый пароль. Сравнительное описание систем OTP (RSA SecurId, сервер одноразовых паролей McAfee и т. д.). RFC 4226 (HOTP) стандарт.
- ✓ • Решение для единого входа Single Sign On. Разница между OpenID и Windows Live ID.

Ход работы:

Первым делом установим само приложение **Rohos Logon Key**

Скачиваю с официального сайта пробную платную версию программы



Two-factor authentication solution, allows you to protect any personal or corporate Windows login with easy-to-use multi-factor authentication. Built-in safeguards prevent 2FA / MFA bypass attacks. Allows protection with a wide variety of cutting-edge MFA methods like OTP, FIDO U2F tokens, Yubikey, smart-cards, RFID or smartphone push. Rohos integrates into conventional password-based Windows login and adds strong MFA control.

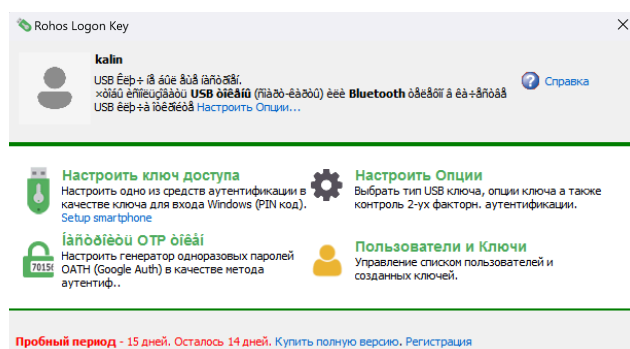
A fully functional 15-day trial

[Download now](#) [Purchase](#)

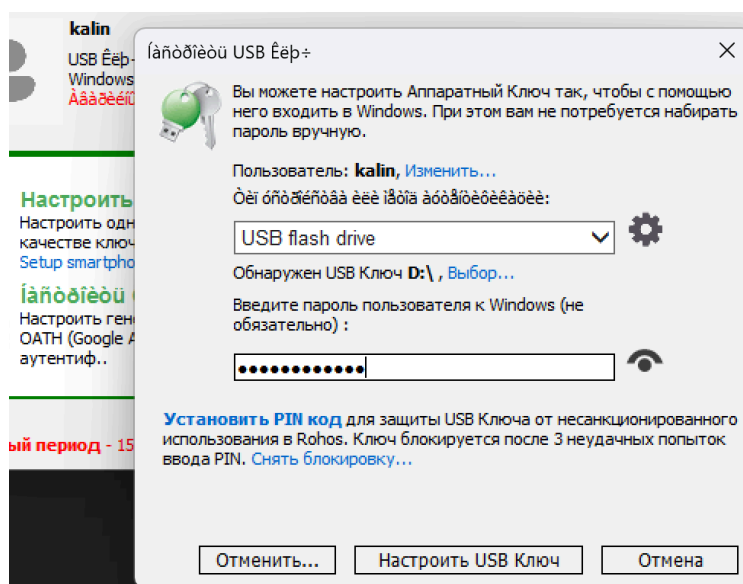
Your Computer security benefits:

- Replaces weak password-based login with a hardware Security Key: USB flash drive, Google Authenticator OTP, FIDO U2F.

после установки открывается окно, где можно выбрать несколько опций



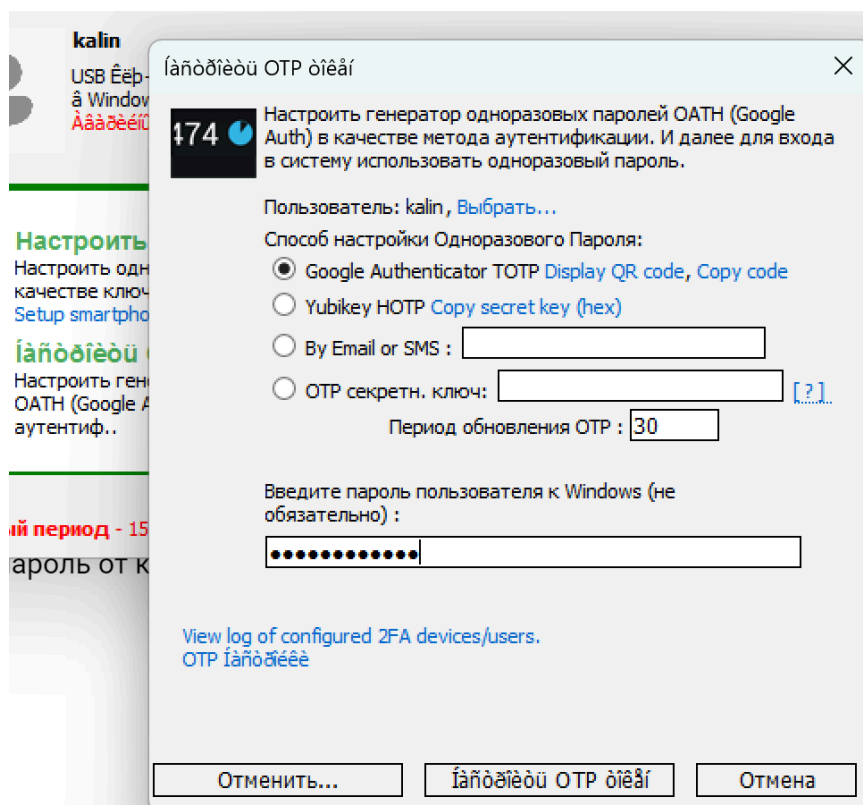
настроим ключ доступа: для этого подключим к компьютеру флешку



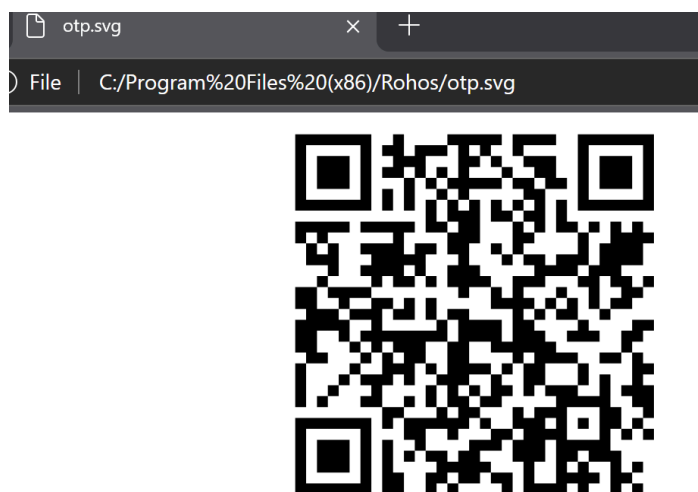
Программа сразу предлагает USB флэш накопитель, но также его можно выбрать нажав на [выбор](#). Также необходимо ввести свой пароль от учетной записи Windows и нажимаем настроить ключ.

После этого при подключении флэшки к ноутбуку не нужно вводить пароль.

Также через это же приложение можно настроить одноразовый пароль от гугл аутентификатора.

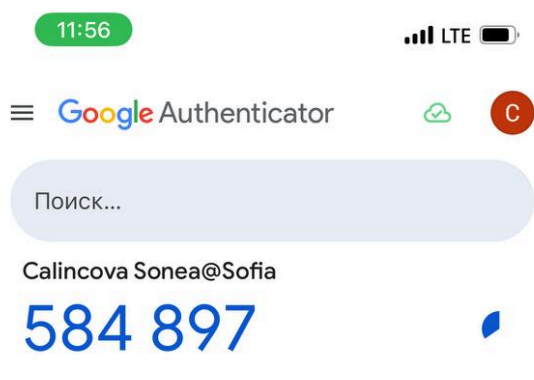


Для этого нажимаем setup otp token, галочкой выбираем гугл аутентификатор вводим пароль от компьютера и выбираем display QR code



открывается новое окно в браузере с нашим QR кодом.

Также необходимо скачать на телефон приложение гугл аутентификатора



В приложении высвечивается одноразовый пароль который меняется каждые 30 секунд.

Теперь можно заходить в учетную запись используя данный одноразовый пароль.

Сравнительное описание систем OTP (RSA SecurID, сервер одноразовых паролей McAfee и т. д.).

Критерий	RSA SecurID	McAfee OTP Server
Тип токенов	Аппаратные или программные токены	Программные токены
Метод генерации паролей	Алгоритм на основе времени и секретного ключа	Алгоритм на основе времени или событий
Поддерживаемые устройства	Смартфоны, компьютеры, аппаратные токены	Смартфоны, компьютеры
Механизм синхронизации	Синхронизация по времени	Синхронизация по времени или событию
Управление пользователями	Интеграция с системами управления пользователями	Интеграция с McAfee ePolicy Orchestrator
Безопасность	Высокий уровень защиты с использованием	Высокий уровень защиты, поддержка нескольких методов

	токенов	
Стоимость внедрения	Более высокая стоимость (аппаратные токены дороже)	Средняя стоимость (программные токены дешевле)

RFC 4226 (HOTP) стандарт

1. Основная идея:

HOTP — это алгоритм для генерации одноразовых паролей (OTP), который использует счетчик и криптографическую хеш-функцию HMAC (Hash-based Message Authentication Code). Каждый новый пароль генерируется на основе увеличенного значения счетчика и секретного ключа.

2. Алгоритм:

- **Секретный ключ (K):** общий секрет между сервером и устройством, известный только двум сторонам.
- **Счетчик (C):** целое число, которое увеличивается с каждым запросом нового одноразового пароля.
- **HMAC-SHA-1:** используется для генерации криптографического хэша.
- **OTP:** одноразовый пароль получается из криптографического хэша путем сокращения его до нужного количества цифр.

3. Генерация OTP:

- Входные данные для генерации: секретный ключ (K) и текущее значение счетчика (C).
- Выполняется HMAC-SHA-1 над секретным ключом и счетчиком:
 $\text{HMAC}(K, C)$.
- Из полученного хэша выбираются определенные байты для генерации финального OTP.
- OTP обычно состоит из 6–8 цифр.

4. Преимущества:

- **Простота интеграции:** HOTP может быть легко внедрен в различные системы аутентификации.
- **Асинхронность:** HOTP не требует синхронизации по времени, в отличие от TOTP (Time-Based OTP), который зависит от времени.
- **Безопасность:** Одноразовые пароли трудно угадать, так как каждый из них основан на криптографическом хэше и уникален для каждого использования.

5. Недостатки:

- **Возможность повторного использования пароля:** если пароль был сгенерирован, но не использован, злоумышленник может его перехватить, если не был увеличен счетчик.
- **Необходимость отслеживания счетчика:** обе стороны должны поддерживать синхронизацию счетчиков. Если счетчик сбивается, это может вызвать проблемы с аутентификацией.

6. Применение:

- HOTP часто используется в системах двухфакторной аутентификации (2FA), где одноразовые пароли отправляются на токены или мобильные устройства для обеспечения дополнительного уровня безопасности.

Разница между OpenID и Windows Live ID

OpenID — это открытый стандарт для децентрализованной аутентификации, который позволяет пользователям использовать один логин для доступа к различным сайтам. Пользователь может выбрать любой провайдер OpenID для управления своими учетными данными.

Windows Live ID (ныне Microsoft Account) — это проприетарная система аутентификации от Microsoft, которая позволяет пользователям использовать

одну учетную запись для доступа к различным сервисам Microsoft, таким как Outlook, OneDrive, и Xbox Live.

Главное различие: **OpenID** — децентрализованная и открытая система, а **Windows Live ID** — централизованная и контролируемая Microsoft.

Библиография

1. <http://www.rohos.com/products/rohos-logon-key/>
2. http://en.wikipedia.org/wiki/One-time_password
3. <http://ru.wikipedia.org/wiki/SecurID>
4. <http://www.mcafee.com/ru/products/one-time-password.aspx#vt=vtab-Overview>
5. <http://ru.wikipedia.org/wiki/HOTP>
6. http://en.wikipedia.org/wiki/Single_sign-on
7. <http://ru.wikipedia.org/wiki/OpenID>
8. http://ru.wikipedia.org/wiki/Windows_Live_ID

ВЫВОД

Rohos Logon Key повышает безопасность за счет одноразовых паролей и USB-ключей, защищая учетные данные от фишинга и взломов, при этом предлагая удобное решение для пользователей с возможностью легкой настройки двухфакторной аутентификации. Программа интегрируется с Active Directory и поддерживает восстановление доступа при утере ключа. Аналогично, RSA SecurID использует двухфакторную аутентификацию с динамически генерируемыми одноразовыми паролями для повышения безопасности доступа. Сервер одноразовых паролей McAfee обеспечивает централизованное управление аутентификацией с одноразовыми паролями, поддерживая широкий набор устройств и приложений для защиты доступа