Государственный Университет Молдовы

Факультет Математики и Информатики

Департамент Информатики

**Лабораторная работа №3**

по курсу “Защита информационных систем”

тема: Многофакторная Аутентификация.

Выполнил студент группы I2302:

Ciobanu Stanislav,

Проверил преподаватель:

Novac.L, doctor conferintiar universitar

Кишинэу, 2024

**Лабораторная работа №3**

**Цель работы**

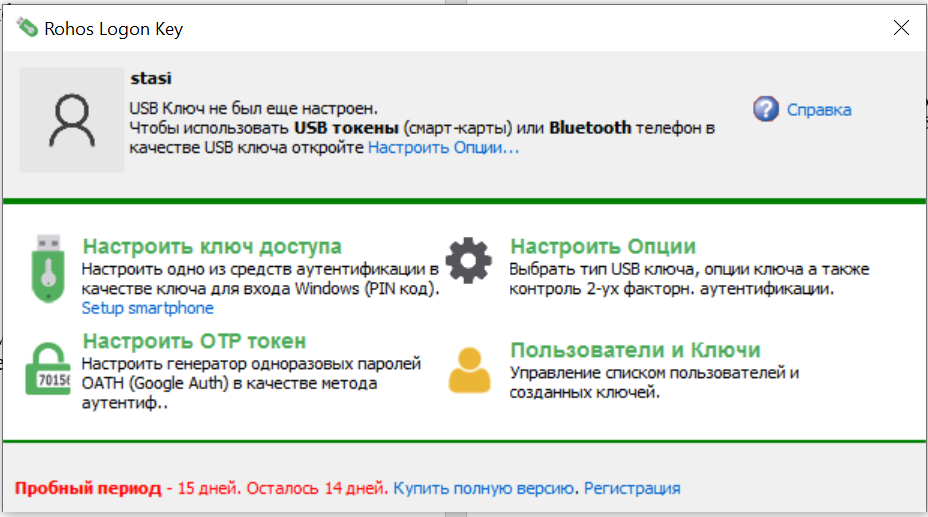
• Создайте токен безопасности с помощью Rohos Logon Key, (Rohos face Logon). • Проверка подлинности Windows с использованием созданного токена безопасности.

• Одноразовый пароль. Сравнительное описание систем OTP (RSA SecurId, сервер одноразовых паролей McAfee и т. д.). RFC 4226 (HOTP) стандарт.

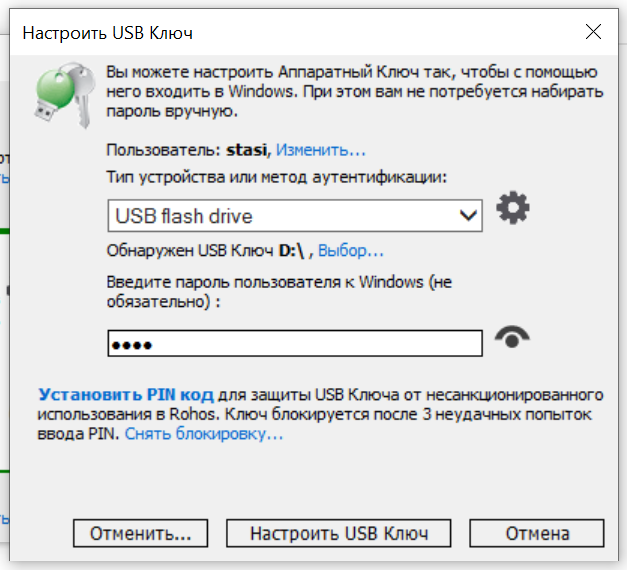
• Решение для единого входа Single Sign On. Разница между OpenID и Windows Live ID

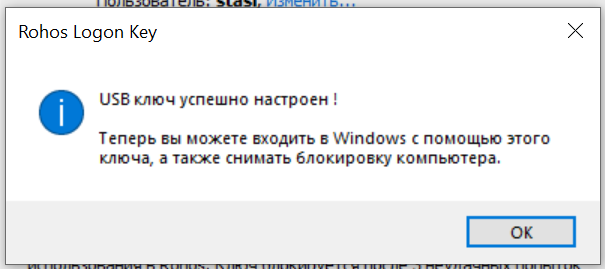
**Начало работы**

Скачаем приложение Rohos Logon Key

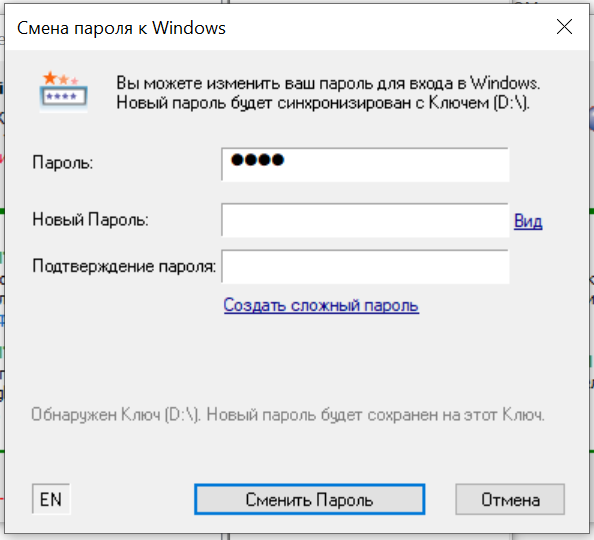
****

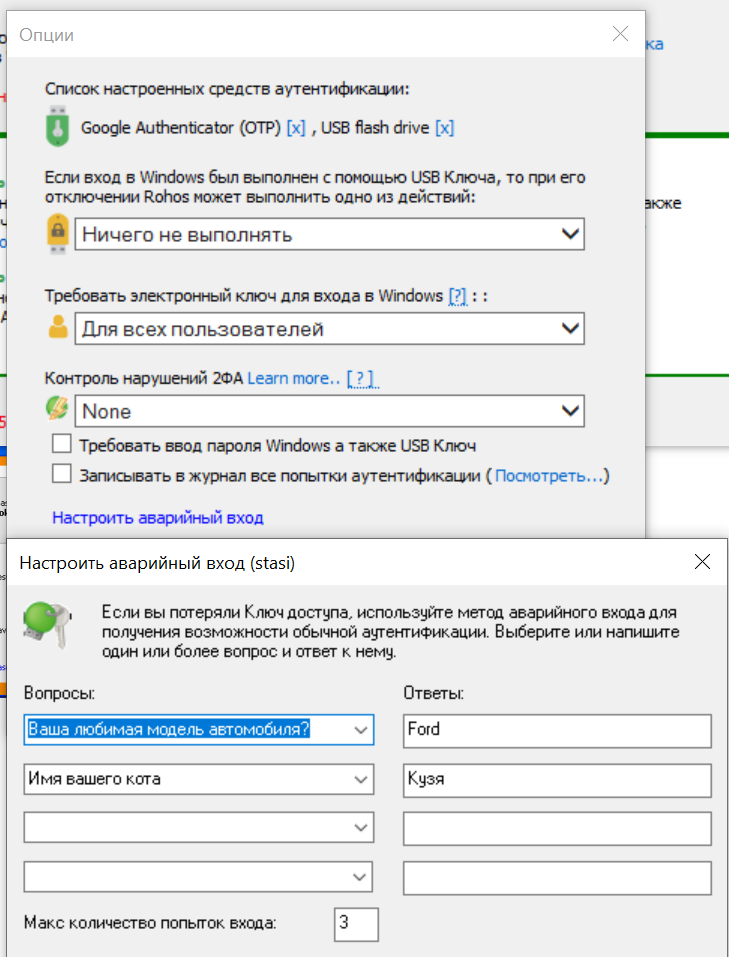
Создадим USB ключ

****

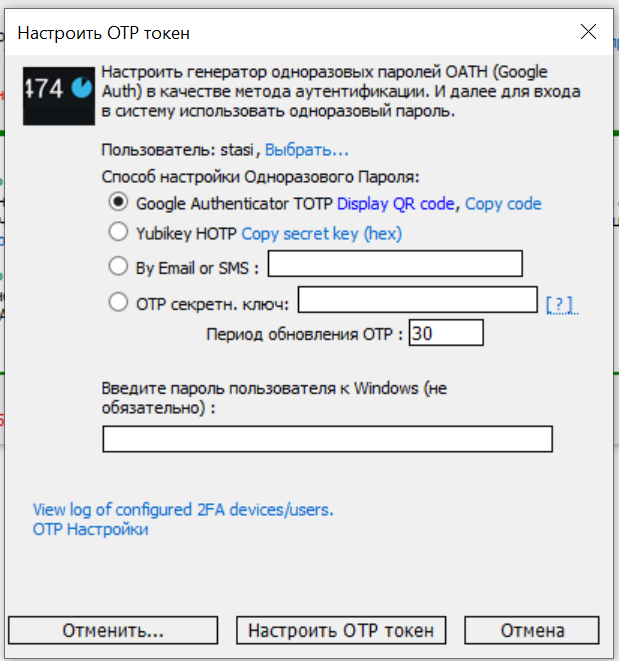
****

Приложение так же позволяет поменять пароль и поменять настройки безопасности. Существует возможность настройки аварийного входа.

****

****

Настроим систему одноразовых паролей через google Authenticator и Email.

****

**Сравнение OpenID и Windows Live ID**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Характеристика** | **OpenID** | | **Windows Live ID** | | --- |  |  | | --- | |  | |
| **Модель аутентификации** | |  | | --- | | Децентрализованная (разные провайдеры) |  |  | | --- | |  | | |  | | --- | | Централизованная (управляется Microsoft) |  |  | | --- | |  | |
| |  | | --- | | **Область применения** |  |  | | --- | |  | | |  | | --- | | Универсальный стандарт для многих сайтов и сервисов |  |  | | --- | |  | | |  | | --- | | Используется для продуктов и сервисов Microsoft |  |  | | --- | |  | |
| |  | | --- | | **Привязка к сервисам** |  |  | | --- | |  | | |  | | --- | | Может использоваться с любыми сервисами, поддерживающими OpenID |  |  | | --- | |  | | |  | | --- | | Используется только для сервисов Microsoft (хотя есть поддержка OpenID Connect для сторонних приложений) |  |  | | --- | |  | |
| **Безопасность** | |  | | --- | | Зависит от провайдера OpenID |  |  | | --- | |  | | |  | | --- | | Обеспечивается Microsoft с поддержкой двухфакторной аутентификации и других технологий безопасности |  |  | | --- | |  | |
| |  | | --- | | **Примеры использования** |  |  | | --- | |  | | |  | | --- | | Вход на различные сторонние веб-сайты (Сервисы Google, GitHub, Yahoo, Steam and e.t.c) |  |  | | --- | |  | | Доступ к сервисам Microsoft: Outlook, OneDrive, Xbox Live и т.д. |

**Выводы**

Приведённые ниже средства защиты не противоречат друг другу и могут быть использованы вместе. При этом каждое средство защиты предоставляет свой способ авторизации. USB ключ предполагает наличие некоего физического предмета для идентификации пользователя. Одноразовые пароли подразумевают аутентификацию через сторонние приложения, номера телефона и.т.п, к которому пользователь имеет доступ.

Наиболее удобным для повседневной жизни я бы назвал аутентификацию через приложение на телефоне т.к этот способ крайне быстр и достаточно безопасен.

OpenID и Windows Live ID предполагают наличие проверенного провайдера и авторизацию через него. Это удобно при работе со связанными сервисами, как те, что предоставляет Microsoft. Один аккаунт на все.