МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ

ДЕПАРТАМЕНТ ИНФОРМАТИКИ

**Лабораторная работа № 3**

**по курсу Securitatea Sistemelor Informatice**

**Тема:**

**Аутентификация на основе нескольких факторов**

Выполнил: Bogdanov Iurii,

студент группы I2302

Проверила: L. Novac,

doctor conferențiar universitar

Кишинёв, 2024

***Введение:***

**Цели 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.

**Rohos Logon Key**

**Типы токенов / символов аутентификации**

* Сетевые устройства с Bluetooth, такие как Pocket PC, Mobile.
* RFID маркировка
* Любая флешка (flash USB)
* USB-токены / смарт-карты: Aladdin eToken PRO, Futu HiToken v22, Aktiv ruToken, uaToken, Crypto Identity 5 и т.д. (USB tokens/smart cards)
* YubiKey и Swekey - токены одноразового пароля
* USB-флешка с отпечатками пальцев, например Transcend, Apacer, LG, TakeMS и т.д.
* Сетевые устройства с Bluetooth, такие как Pocket PC, Mobile.
* RFID маркировка.

**Rohos Logon Key** - решение для проверки подлинности преобразует любой USB-накопитель в токен безопасности для вашего компьютера и обеспечивает доступ к Windows в режиме защищенного USB-токена, заменяя вход в Windows.

**Определить преимущества безопасности для собственного компьютера**

**Решение для одноразового пароля** (**One-Time Password** / **OTP), генерация OTP, доставка OTP.**

* One Time Password через SMS
* One Time Password (Пароль на мобильном телефоне)
* Веб-методы (Web-based methods)

**RSA SecurID**

**Методы аутентификации, основанные на бизнес-потребностях и других требованиях**

**Решение Single Sign One *(SSO)*. Разница между OpenID и** Windows Live ID.

/ Преимущества / Недостатки / Безопасность

**Windows Live ID.** Рабочий механизм *Windows Live ID*

***Ход работы:***

**Rohos Logon Key** — это программа, предназначенная для повышения безопасности компьютера, предоставляя возможность использовать USB-устройства или смарт-карты для аутентификации в Windows вместо традиционного пароля. Программа позволяет превратить любое USB-устройство в безопасный ключ для доступа к компьютеру. Также совместимо с RFID, OTP, U2F-токенами, заменяя пароль для входа в систему Windows.

**Преимущества использования Rohos Logon Key для безопасности компьютера:**

*1. Повышенная защита от несанкционированного доступа:*

Вместо пароля используется физический токен, такой как USB-накопитель или смарт-карта. Это означает, что злоумышленник не сможет войти в систему без доступа к устройству, даже если узнает ваш пароль.

Возможность добавления PIN-кода к USB-устройству создаёт дополнительный уровень защиты, требуя от пользователя как устройства, так и кода для входа.

*2. Автоматическая блокировка при отключении токена:*

Rohos Logon Key может настроить систему на автоматическое блокирование экрана при отключении токена. Это удобно и обеспечивает мгновенную защиту, если вы покидаете компьютер, случайно оставив его разблокированным.

Также можно настроить автоматическую блокировку через определённое время бездействия, что предотвращает несанкционированный доступ, если вы отошли от компьютера.

*3. Снижение зависимости от паролей:*

Отсутствие необходимости ввода пароля при каждом входе помогает избежать угрозы перехвата или кражи паролей через вредоносные программы или методы, такие как кейлоггеры.

Защита от фишинга и поддельных страниц: использование физического устройства исключает риск ввода пароля на поддельных веб-сайтах.

*4. Удобство использования:*

Использование USB-устройства позволяет входить в систему быстро и легко, избавляя от необходимости запоминать и вводить длинные и сложные пароли.

Программа поддерживает множество типов устройств: USB-флешки, смарт-карты, устройства с Bluetooth и RFID, что позволяет выбрать наиболее удобный вариант для вашего образа жизни или рабочего процесса.

*5. Интеграция с корпоративными системами:*

Rohos Logon Key поддерживает интеграцию с Active Directory, что позволяет администраторам централизованно управлять безопасностью и доступом сотрудников к корпоративным данным.

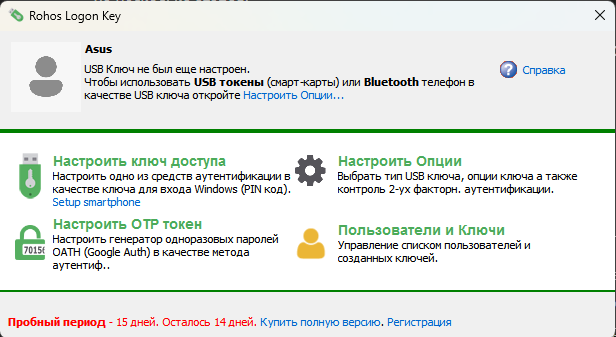
В корпоративной среде использование USB-токенов может обеспечить более высокий уровень контроля доступа к чувствительным данным и снижает риск несанкционированного доступа.

*6. Резервные функции для предотвращения потери доступа:*

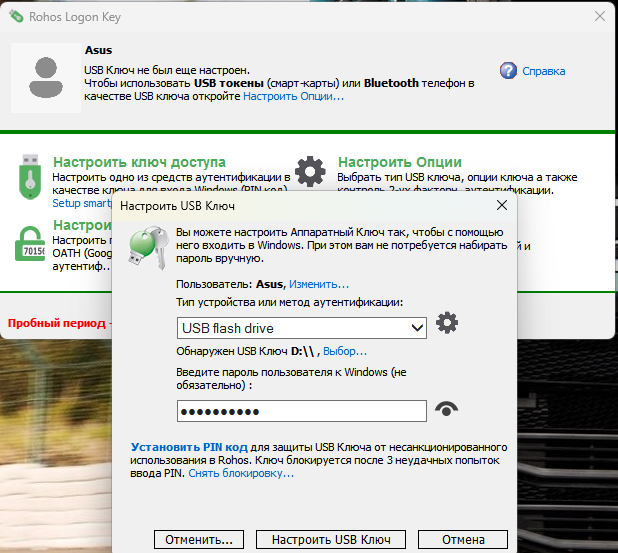
Программа поддерживает создание резервного пароля и резервного копирования настроек, что позволит восстановить доступ в случае потери или повреждения USB-токена.

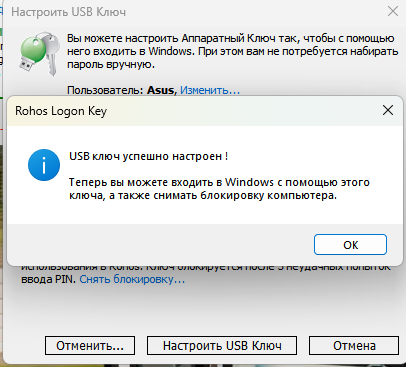
В случае, если токен утерян или поврежден, это позволяет восстановить доступ к системе, не нарушая общую безопасность.

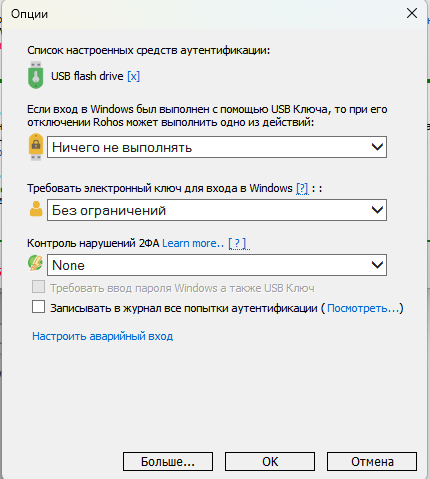
**Главное меню утилиты Rohos Logon Key**



Теперь необходимо настроить USB ключ, нажав на “Настроить ключ доступа” у нас открывается следущее меню, в котором мы выбираем свою флешку и вводим пароль от устройства. После этого нажимаем “ Настроить USB ключ”.



Видим, что настройка была выполнена успешно!

Также в этом приложение мы можем настроить и дополнительные опции по своему желанию.

После выполнения настройки USB ключа данная флешка может быть использована для входа в профиль без ввода пароля в ручную. Такая возмозможность является удобной для пользователя при использовании флешки постоянно.

***Сравнительное описание систем OTP (RSA SecurId, сервер***

***одноразовых паролей McAfee и т. д.). RFC 4226 (HOTP) стандарт:***

**RSA SecurID:**

RSA SecurID — решение двухфакторной аутентификации от RSA Security (Dell Technologies), которое повышает безопасность доступа к системам, требуя не только пароль, но и одноразовый пароль (OTP), генерируемый физическим или виртуальным токеном.

**Ключевые особенности:**

*Физические и виртуальные токены:* Поддерживает аппаратные токены с дисплеем и программные токены для смартфонов, что позволяет гибко применять решение в разных средах.

*Одноразовые пароли (OTP):* Токены генерируют пароли, действительные в течение короткого времени, обновляющиеся каждую минуту, что защищает от перехвата.

*Широкая интеграция:* Совместим с протоколами RADIUS и другими, что позволяет использовать SecurID в VPN, облачных сервисах и корпоративных приложениях.

*Адаптивная аутентификация:* Учитывает контекст использования (например, местоположение и устройство), чтобы автоматически повышать уровень безопасности при необходимости.

*Многофакторность:* Комбинирует OTP с паролем или другими методами, такими как биометрия, для усиленной защиты.

RSA SecurID используется в корпоративных и государственных структурах благодаря своей надежности и гибкости в настройке.

**Сервер одноразовых паролей McAfree:**

McAfee One Time Password Server — это решение для многофакторной аутентификации, разработанное компанией McAfee (подразделение Intel Security). Оно предоставляет дополнительный уровень защиты, требуя от пользователя ввода одноразового пароля (OTP) в дополнение к основному паролю для подтверждения подлинности при доступе к системе.

**Ключевые особенности:**

*Гибкость в выборе токенов:* McAfee OTP Server поддерживает различные методы генерации одноразовых паролей, такие как SMS, электронная почта, мобильные приложения и аппаратные токены. Это позволяет организациям выбирать удобный способ для пользователей.

*Пользовательские настройки:* Администраторы могут настраивать политику для токенов, определяя частоту обновления паролей и время их действия. Это обеспечивает дополнительную адаптивность под потребности безопасности.

Широкие возможности интеграции: Поддерживает стандартные протоколы аутентификации, такие как RADIUS и LDAP, что позволяет легко интегрировать решение с различными корпоративными системами и приложениями.

*Адаптивная аутентификация:* Система анализирует контекст использования, такой как местоположение, время суток и другие параметры, что позволяет адаптировать уровень безопасности в зависимости от условий.

Удобство использования для сотрудников: Возможность получения одноразового пароля через SMS, email или приложение упрощает процесс авторизации и снижает нагрузку на IT-отдел.

McAfee One Time Password Server — это надежное решение для организаций, требующих повышенного уровня безопасности, особенно в корпоративной среде.

**Сходства и различия RSA SecurID и McAfee:**

**Сходства:**

*Многофакторная аутентификация:* Оба используют пароли и одноразовые пароли (OTP) для защиты.

*Интеграция:* Поддерживают RADIUS и легко интегрируются с корпоративными системами.

Адаптивная аутентификация: Учитывают контекст (местоположение, время) для повышения безопасности.

**Различия:**

*Тип токенов:* RSA SecurID использует физические и программные токены, McAfee поддерживает OTP через SMS, email и мобильные приложения.

*Целевая аудитория:* RSA SecurID больше ориентирован на крупные компании и государственные учреждения, McAfee подходит для компаний разного масштаба.

*Генерация OTP:* RSA использует синхронизацию по времени (TOTP), McAfee предлагает различные методы доставки, включая SMS и email.

Масштабируемость: RSA требует инфраструктуры для управления токенами, тогда как McAfee более гибок и масштабируем с поддержкой облака.

RSA SecurID лучше подходит для крупных предприятий, а McAfee OTP Server — для гибкости и удобства настройки.

**Стандарт RFC 4426(HOTP) – HMAC-Based One-Time Password Algorithm:**

Стандарт RFC 4226 (HOTP) – HMAC-Based One-Time Password Algorithm

HOTP (HMAC-Based One-Time Password) — это алгоритм для создания одноразовых паролей (OTP), работающий на основе технологии HMAC (Hash-based Message Authentication Code). RFC 4226 описывает протокол, определяющий, как HOTP должен функционировать.

**Основные компоненты:**

*Секретный ключ* — это уникальный ключ, который известен как клиенту (например, устройству пользователя), так и серверу. Он служит основой для генерации OTP посредством хэширования.

*Счетчик* — параметр, который увеличивается при каждой успешной аутентификации. Обычно он начинает отсчет с нуля и синхронизируется между сервером и клиентом при каждом входе.

*Хэш-функция* — один из основных элементов безопасности HOTP. В спецификации обычно указана SHA-1, но также возможно использовать более современные хэш-алгоритмы, такие как SHA-256.

*Длина OTP* — определяет количество цифр в одноразовом пароле, которое часто составляет 6 символов.

**Процесс генерации OTP:**

*Хэширование:* HMAC создается с использованием секретного ключа и текущего значения счетчика.

*Обработка:* Полученное хэш-значение может быть усечено для получения требуемой длины OTP, которая затем обрабатывается в числовое значение.

**Процесс проверки OTP:**

*Генерация сервером:* Сервер повторяет процесс генерации OTP, используя тот же секретный ключ и значение счетчика.

*Сравнение:* OTP, созданный сервером, сравнивается с тем, который предоставил пользователь. Если значения совпадают, аутентификация проходит успешно.

*Обновление счетчика:* При успешной проверке счетчик на сервере увеличивается, чтобы быть готовым для следующей аутентификации.

**Особенности и преимущества:**

Генерация уникальных OTP обеспечивает защиту от повторного использования паролей и различных видов атак.

Алгоритм легок в реализации и демонстрирует высокую производительность.

HOTP основан на хорошо изученных криптографических методах, таких как HMAC и хэш-функции, что делает его надежным.

Стандарт универсален и широко применяется для защиты доступа в разнообразных системах, от систем входа до подтверждения транзакций.

RFC 4226 — это общедоступный стандарт, что способствует его повсеместному использованию и внедрению различными поставщиками. Алгоритм HOTP широко используется в приложениях для двухфакторной аутентификации.

**Single Sign-On (SSO)**

Единая система входа (SSO) позволяет пользователю входить в различные приложения и ресурсы с помощью одного набора учетных данных. Это избавляет пользователя от необходимости повторной аутентификации при доступе к другим системам после первого входа.

**OpenID**

OpenID — это открытый протокол аутентификации, который предоставляет пользователям возможность использовать один идентификатор для входа на различные сайты. OpenID позволяет входить без создания нового аккаунта на каждом сайте, используя вместо этого учетную запись у провайдера OpenID. Стандарт независим от платформы и предоставляет пользователям возможность выбора поставщика OpenID, например, Google или Yahoo.

**Windows Live ID**

Windows Live ID (также известен как Microsoft Account) представляет собой учетную запись, используемую для доступа к сервисам и продуктам Microsoft, таким как Outlook, OneDrive, Skype и другим. Windows Live ID тесно связан с продуктами Microsoft и предоставляет единый вход для экосистемы продуктов компании. Хотя его можно использовать на сторонних сайтах, он в первую очередь предназначен для интеграции в продукты Microsoft. С помощью Windows Live ID можно легко получить доступ к почтовому ящику, облачному хранилищу и многим другим сервисам.

**Общие черты OpenID и Windows Live ID:**

* Оба являются формами SSO, позволяя пользователям входить в различные сервисы без необходимости постоянной повторной аутентификации.
* OpenID и Windows Live ID упрощают процесс входа для пользователей, избавляя их от необходимости запоминать множество паролей.

**Различия между OpenID и Windows Live ID:**

OpenID является открытым стандартом SSO и может использоваться с различными провайдерами, тогда как Windows Live ID — это идентификатор, предназначенный в основном для продуктов и сервисов Microsoft.

**Вывод:**

**Rohos Logon Key** — это решение для единого входа (Single Sign-On) с использованием USB-ключа в качестве физического токена. Оно обеспечивает двухфакторную аутентификацию, сочетая учетные данные пользователя с наличием физического ключа.

**OTP** (одноразовый пароль) представляет собой метод аутентификации, при котором генерируется пароль, действительный в течение ограниченного времени. Он может применяться как самостоятельный метод аутентификации или в сочетании с другими способами для повышения уровня безопасности.

**HOTP** — это разновидность OTP, использующая алгоритм HMAC для создания одноразовых паролей. Этот подход добавляет дополнительную защиту благодаря использованию криптографической хэш-функции.

**OpenID** — это протокол аутентификации с открытым исходным кодом, который позволяет пользователям использовать один идентификатор для доступа к различным веб-сайтам, что облегчает единый вход без создания новых учетных записей.

**Windows Live ID (Microsoft Account)** — это учетная запись от Microsoft, предоставляющая единый идентификатор для входа в экосистему продуктов Microsoft, таких как Outlook, OneDrive и Skype.

Все перечисленные методы добавляют дополнительные уровни безопасности за счет многофакторной аутентификации, снижая вероятность несанкционированного доступа. Такие методы, как OTP и HOTP, защищают от фишинга, так как даже при утечке пароля злоумышленнику потребуется либо физический токен, либо сгенерированный одноразовый пароль.

Решения, подобные Rohos Logon Key, обеспечивают баланс между безопасностью и удобством для пользователя, что особенно важно для повседневного использования. Большинство описанных методов используют многофакторную аутентификацию (MFA), которая делает процесс входа в систему более защищенным.

Применение стандартов безопасности, таких как HMAC в HOTP, или использование открытых протоколов, как в OpenID, способствует созданию надежных механизмов аутентификации.

Выбор подходящего метода аутентификации определяется конкретными требованиями, уровнем безопасности и удобством для пользователей. Например, OpenID может использоваться для упрощенного единого входа, тогда как Rohos Logon Key подойдет для физической аутентификации на устройстве.

В конечном итоге выбор подходящего метода аутентификации зависит от уровня безопасности и удобства, которые требуются для конкретного приложения или ситуации.

**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](http://www.mcafee.com/ru/products/one-time-password.aspx" \l "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>