МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«Российский государственный гидрометеорологический университет»
(РГГМУ)

Кафедра информационных технологий и систем безопасности

И.В. Ананченко, П.И. Смирнов, Ю.М. Шапаренко

АППАРАТНЫЕ КЛЮЧИ ETOKEN. СРЕДСТВО ЗАЩИТЫ ETOKEN NETWORK LOGON

Методические указания

Санкт- Петербург
2015

УДК 681.3.657.1

Ананченко И.В., Смирнов П.И., Шапаренко Ю.М. Аппаратные ключи eToken. Средство защиты eToken Network Logon. – СПб.: изд. РГГМУ, 2015. – 30 с.

В методических указаниях к лабораторной работе рассматривается вопросы работы с аппаратными ключами серии eToken (установка, обслуживание и администрирование), развертывание и использование eToken Network Logon. Работа ориентирована на приобретение студентами навыков установки и эксплуатации программно-аппаратного решения eToken Network Logon, предназначенного для кардинального решения проблемы «слабых» паролей при работе на компьютерах под управлением Microsoft Windows. Методические указания соответствует содержанию дисциплин «Информационная безопасность телекоммуникационных систем», «Программно-аппаратные средства обеспечения информационной безопасности», «Защита информации» государственных образовательных стандартов ФГОС 3+. Позволяют формировать общепрофессиональные компетенции (ПК-2,11,12) по направлению подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем». ПК-2-способность применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач. ПК-11-способность осуществлять подбор, изучение, анализ и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем. ПК-12 - способность применять современные методы исследования с использованием компьютерной техники.

Методические указания предназначены для студентов и аспирантов высших учебных заведений и могут быть использованы в системах непрерывного профессионального образования специалистов по компьютерным технологиям.

Ил.9, библиогр. 13 назв., ПК-2,11,12.

Рецензент: В.А. Холоднов, д.т.н., профессор кафедры системного анализа СПбГТИ (ТУ)

Утверждено на заседании учебно-методической комиссии факультета информационных систем и геотехнологий РГГМУ __.__.2015

Рекомендовано к изданию РИО РГГМУ

Введение

В процессе жизнедеятельности человека его опыт как накапливающаяся в огромном количестве субъективная и объективная информация может быть зафиксирован, сохранен и передан другим людям. Исторический аспект рассмотрения проблемы накопления информации позволяет вскрыть наиболее значимые для человечества проблемы и закономерности, проследить динамику информационного развития. Современный этап информационного развития общества характеризуется быстрой сменой технологий и появлением новых сетевых архитектур. Вследствие этого возникают большие объемы управляющей информации, которые необходимо обеспечивать защитой. Концентрация информации в компьютерных системах вынуждает наращивать усилия по её защите. Соответственно, с появлением новых технологий появляются новый виды угроз и нарушителей. В этих условиях защите информации от несанкционированного доступа в последнее время отводится весьма значительное место, в том числе и на предприятиях различных отраслей промышленности Российской Федерации.

В государственном стандарте ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию» [1] перечислено большое количество угроз, которые могут привести к нарушению ее конфиденциальности, целостности и доступности существенный ущерб информации при воздействии на компьютерную систему. От угроз безопасности информации, таких как несанкционированный доступ злоумышленников, деятельность технических разведок и злой умысел сотрудников (инсайдеров), можно защититься, только используя эшелонированную защиту. Организация защиты информации направлена на предотвращение утечки защищаемой информации по техническим каналам (т.е. «естественным» путем за счет излучений и наводок), а также на защиту от несанкционированных и непреднамеренных воздействий нарушителей.

Система защиты информации представляет собой совокупность технических, программных, программно-технических средств защиты информации и средств контроля эффективности защиты информации, а также организационных мер защиты. Модели безопасности и защиты информации от различных видов угроз и нарушителей, а также разработанные организационно-технические мероприятия, аппаратно-программные и технические методы для защиты информации на конкретном предприятии представляются в документе «Политика информационной безопасности», который утверждается руководителем предприятия. При организации безопасности информации на предприятии большое внимание уделяется защите от несанкционированного доступа (НСД). В руководящем документе «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» [2] отражены основные требования по организации защиты, которые необходимо учитывать при разработке «Политики информационной безопасности» для защиты автоматизированных систем организации. Для защиты информации от НСД необходимо выполнить следующие требования:

- ограничение физического доступа к АС,
- идентификация и аутентификация пользователей,
- ограничение доступа на вход в систему,
- разграничение доступа,
- регистрация событий (аудит),
- криптографическая защита,
- контроль целостности, включая периодическое тестирование средств защиты,
- управление политикой безопасности,
- уничтожение остаточной информации (очистка при завершении процесса),
- антивирусная защита,

- восстановление данных,
- при удаленном взаимодействии - сетевая защита,
- защита от утечки и перехвата информации по техническим каналам.

В зависимости от модели угроз и нарушителей применяются различные средства защиты информации. Программно-аппаратные средства защиты информации – это средства защиты информации, которые наиболее полно выполняют меры и соответствующие им методы по противодействию НСД.

Использование программно-аппаратных средств защиты позволяет реализовывать схемы защиты, более устойчивые к воздействию злоумышленника, чем использование традиционных чисто программных средств защиты [3]. Например, с помощью аппаратных ключей защиты серий eToken и ruToken (”токенов”) можно реализовать схемы однофакторной (наличие аппаратного токена у пользователя достаточно для доступа к системе) или двухфакторной защиты (наличие аппаратного токена у пользователя позволяет пользователю получить доступ к системе, только в том случае, если пользователь введет корректный pin-код, дающий ему право работать с аппаратным токеном).

Снижение стоимости аппаратных ключей защиты позволяет более широко использовать их для организации разных схем защиты данных пользователей и программного обеспечения. Аппаратные ключи защиты (токены) можно классифицировать с использованием различных критериев классификации (например, назначение, объем защищенной памяти, реализованный в устройстве, аппаратно поддерживаемые ключом алгоритмы шифрования, производитель средств защиты и т.д.). Одна из возможных классификационных схем по назначению включает в себя классификационные группы: 1) для защиты программного обеспечения от несанкционированного использования (например, ключи серий HASP или GUARDANT); 2) группа ключей, предназначенная для хранения и обработки конфиденциальной информации пользователей (например, ключи серий eToken или RuToken – хранение электронных цифровых сертификатов, средства поддержки

электронной-цифровой подписи, хранение конфиденциальной информации – пароли, pin-коды и т.д.). Деление на названные две группы достаточно условное, т.к. все устройства имеют защищенную память для хранения конфиденциальных данных и реализованные на аппаратном уровне средств шифрования. Однако для первой группы (защита программного обеспечения) характерно наличие специального программного обеспечения (комплект разработчика), позволяющего максимально просто защищать программное обеспечение. Ключи, относящиеся ко второй классификационной группе, распознаются операционной системой как устройства для чтения смарт-карт, с вставленной в устройство смарт-картой, что позволяет использовать не только программное обеспечение, разработанное для конкретного устройства, но и программное обеспечение поддерживающее работу с устройствами для чтения смарт-карт.

Линейка USB-ключей и смарт-карт eToken включает в себя устройства, выполняющие базовые функции безопасности, а также комбинированные продукты, сочетающие в себе возможности нескольких устройств. Решения, основанные на использовании ключей eToken, выбрали свыше 75% ведущих российских заказчиков [4]: средние и крупные компании, предприятия с распределённой структурой, кредитные и банковские организации, телекоммуникационные компании и сервис-провайдеры, медицинские и страховые учреждения, государственные и налоговые органы, удостоверяющие центры и операторы электронной отчетности.

Теоретическая часть. Знакомство с аппаратными ключами защиты серии eToken

Общая характеристика ключей eToken: электронные USB-ключи и смарт-карты eToken представляют собой компактные устройства, предназначенные для обеспечения информационной безопасности корпоративных заказчиков и частных пользователей. Устройства eToken содержат процессор и модули

памяти, функционирующие под управлением своей операционной системы, выполняют необходимые прикладные программы и хранят информацию.

Использование продуктов eToken помогает решить следующие типовые задачи обеспечения безопасности:

- обеспечение процесса двухфакторной аутентификации на локальном компьютере и в корпоративной сети, защищенный доступ к бизнес-приложениям;
- шифрование данных на серверах, ноутбуках, рабочих станциях;
- обеспечение защиты персональных данных;
- защита электронной почты, защита информации в системах электронного документооборота;
- обеспечение безопасности финансовых операций в системах дистанционного банковского обслуживания (ДБО);
- внедрение электронной цифровой подписи (ЭЦП) и защиты документов в системах сдачи электронной отчетности через Интернет;
- обеспечение защиты корпоративных сайтов в сети Интернет.

Модельный ряд активно используемых в настоящее время ключей серии eToken [5] включает в себя 7 типов устройств: eToken ГОСТ, eToken PRO (Java), КриптоПро eToken CSP, eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken PASS, eToken PRO Anywhere. Типы можно распределить по трем группам:

1. USB-ключи и смарт-карты,
2. комбинированные USB-ключи,
3. специализированные USB-ключи.

Группа 1. **USB-ключи и смарт-карты** – четыре модели.

Электронный ключ **eToken ГОСТ**:

- средство формирования электронной подписи (ЭЦП) по алгоритму ГОСТ Р 34.10-2001;
- рекомендуется для применения в системах ДБО, юридически-значимого документооборота, Web-сервисах;
- сертифицирован ФСБ России.

Электронный ключ **eToken PRO (Java)**:

- рекомендуемая производителем модель, подходящая для большинства вариантов использования;
- увеличенный объем защищенной памяти для хранения пользовательских данных (72 Кб);
- расширение функционала за счет загрузки Java-апплетов;
- сертифицирован ФСТЭК России.

Электронный ключ **КриптоПро eToken CSP**:

- средство формирования электронной подписи (ЭЦП) с поддержкой СКЗИ КриптоПро CSP;
- защищенный обмен между аппаратным ключом eToken и программными компонентами КриптоПро CSP (функциональный ключевой носитель - ФКН).

Группа 2. **Комбинированные USB-ключи** – три модели.

Электронный ключ **eToken NG-FLASH (Java)** – представляет собой комбинированный токен, сочетающий возможности средства аутентификации и переносного защищенного накопителя данных, аппаратно поддерживающего работу с цифровыми сертификатами и электронно-цифровой подписью (ЭЦП). Для процедуры двухфакторной аутентификации пользователя с применением

электронного ключа eToken NG-FLASH (Java), возможно использование в качестве второго критерия идентификации:

- цифровых сертификатов стандарта X.509;
- паролей, кодов доступа и других данных, хранящихся в защищенной памяти токена, что позволяет электронному ключу работать на различных программных и аппаратных платформах и с различными приложениями.

Электронный ключ eToken NG-FLASH (Java) может использоваться, как защищенный накопитель данных – дополнительная память токена максимальным объемом до 16 Гб позволяет хранить данные в зашифрованном виде и может быть использована для:

- доверенной загрузки операционных систем Microsoft Windows или Linux (образ операционной системы записывается в память устройства);
- хранения и запуска предварительно сконфигурированной виртуальной машины (VMWare, Virtual PC) с предустановленным набором программного обеспечения и настроенными параметрами безопасности;
- автоматического запуска приложений из памяти устройства;
- безопасного хранения, транспортировки и резервного копирования данных;
- запуска безопасного предварительно настроенного браузера.

С помощью утилиты eToken NG-FLASH Partition Application дополнительную Flash-память устройства можно разметить на две области — доступную только для чтения ROM-область и перезаписываемую область. В ROM-область можно предустановить необходимые пользователю приложения, определить конфигурационный файл для их автозапуска. В этом случае при подсоединении электронного ключа к компьютеру дополнительная Flash-память будет распознана как два логических диска, с одного из которых, представляющего ROM-область, будет произведен автоматических запуск приложений. Данные в перезаписываемой области хранятся в зашифрованном

виде. Для шифрования используется алгоритм AES с длиной ключа 256 бит. При считывании данные расшифровываются «на лету». Когда происходит запись или сохранение – данные зашифровываются незаметно для пользователя. При необходимости дополнительная Flash-память токена может быть перераспределена между областями и инициализирована заново самим пользователем. Следует учитывать, что при перераспределении областей происходит потеря текущего содержимого каждой из областей.

Возможности **eToken NG-FLASH** могут использоваться для обеспечения двухфакторной аутентификации пользователей в системах, построенных на основе технологии PKI, в унаследованных приложениях, на рабочих станциях и в сети, в гетерогенных средах, при удаленном доступе к информационным ресурсам. Устройство поддерживает аппаратную реализацию алгоритмов шифрования RSA/2048, RSA/1024, DES, 3DES, SHA-1. eToken NG-FLASH можно использовать в системах PKI с поддержкой программных интерфейсов Microsoft CryptoAPI и PKCS#11. На электронный ключ eToken NG-FLASH (Java) может быть предустановлена операционная система Microsoft Windows PE, служащая для последующей установки Windows на сервере или настольном компьютере и устранения неполадок, а также различные дистрибутивы Linux. В этом случае загрузка компьютера будет произведена с хранящегося в памяти ключа образа операционной системы. Для аутентификации пользователя в уже загруженной операционной системе могут использоваться регистрационные имя пользователя и пароль, либо цифровой сертификат стандарта X.509 и закрытый ключ, хранящиеся в защищенной памяти микросхемы смарт-карты.

Электронный ключ eToken NG-FLASH (Java) может быть использован для доверенной загрузки терминальных клиентов. В этом случае образ операционной системы для терминального клиента располагается в ROM-области токена, а аппаратная конфигурация терминального клиента может быть удешевлена за счет исключения модуля Flash-памяти на материнской плате устройства. Для обеспечения дополнительного уровня безопасности данные,

хранящиеся в перезаписываемой области, могут быть зашифрованы встроенным алгоритмом шифрования AES-256 или, например, с использованием приложений линейки Secret Disk. Приложения, установленные в ROM-области электронного ключа eToken NG-FLASH (Java), могут запускаться автоматически при подсоединении токена к компьютеру. Примерами таких приложений могут быть:

- программа установки драйверов eToken;
- приложения безопасности, использующие возможности eToken (VPN-клиент, программы шифрования дисков и др.);
- файлы установки и др.

Электронный ключ **eToken NG-OTP (Java)** – комбинированный USB-ключ с генератором одноразовых паролей, не требующий подключения к компьютеру. Устройство представляет собой комбинированный токен, сочетающий возможности средства аутентификации и генератора одноразовых паролей (OTP), аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭЦП). Для двухфакторной аутентификации пользователя с применением электронного ключа eToken NG-OTP (Java) возможно использование в качестве второго критерия идентификации:

- цифровых сертификатов стандарта X.509;
- одноразовых паролей (OTP);
- паролей, кодов доступа и других данных, хранящихся в защищенной памяти токена, что позволяет электронному ключу работать на различных программных и аппаратных платформах и с различными приложениями.
- Используя генератор одноразовых паролей eToken NG-OTP (Java), Вы можете организовать безопасный доступ к корпоративным ресурсам без установки дополнительного клиентского программного обеспечения и без физического подключения токена к компьютеру.

eToken NG-OTP (Java) расширяет спектр аппаратных платформ и операционных систем, на которых возможно использование электронных ключей eToken, так как с этим ключом можно работать с портативными компьютерами, смартфонами, а также обычными компьютерами, на которых отсутствуют или недоступны USB-порты. При использовании устройства в режиме генератора одноразовых паролей сгенерированный одноразовый пароль отображается на дисплее токена и может быть введен в компьютер через клавиатуру или перьевой ввод, т.е. не требуется подключать eToken NG-OTP (Java) к чему-либо. Функционально eToken NG-OTP (Java) аналогичен USB-ключу eToken PRO (Java) и дополнительно оснащен кнопкой и дисплеем для отображения сгенерированных одноразовых паролей, а также имеет встроенные элементы питания и световой индикатор режимов работы.

Электронный ключ **eToken PASS** – автономный генератор одноразовых паролей, не требует подключения к компьютеру и установки дополнительного программного обеспечения. eToken PASS можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации RADIUS – VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и др. Комплект разработчика eToken OTP SDK 2.0 позволяет добавить поддержку аутентификации по одноразовым паролям в собственные приложения.

Основные преимущества использования eToken PASS:

- Не требует установки дополнительного клиентского ПО.
- Не требует установки драйверов.
- Работает без подключения к компьютеру – нет необходимости наличия свободного USB-порта.
- Обеспечивает возможность работы в любой операционной системе.
- Обеспечивает возможность работы с мобильных устройств.
- Одноразовый пароль действует только в течение одного сеанса связи – пользователь не должен беспокоиться о том, что используемый в

настоящий момент пароль может быть подсмотрен или перехвачен злоумышленником.

- Относительно низкая цена устройства.

Принцип работы eToken PASS – реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP), разработанный в рамках инициативы OATH. Алгоритм основан на алгоритме HMAC и хэш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе eToken TMS. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере – при каждой удачной аутентификации по OTP. При запросе на аутентификацию проверка OTP осуществляется сервером RADIUS (Microsoft IAS, FreeRadius и др.), который обращается к системе eToken TMS, осуществляющей генерацию OTP на стороне сервера. Если введенное пользователем значение OTP, совпадает со значением, полученным на сервере, аутентификация считается успешной, и RADIUS сервер отправляет соответствующий ответ. Партия устройств eToken PASS поставляется с зашифрованным файлом, содержащим начальные значения для всех устройств партии, данный файл импортируется администратором в систему eToken TMS. После этого для назначения устройства пользователю необходимо ввести серийного номера устройства (напечатан на корпусе).

В случае нарушения синхронизации счетчика генерации в устройстве и на сервере, система eToken TMS позволяет восстановить синхронизацию, т.е. привести значение на сервере в соответствие значению, хранящемуся в устройстве. Для этого администратор системы или сам пользователь (при наличии соответствующих разрешений) должен сгенерировать два последовательных значения OTP и отправить их на сервер через Web-интерфейс eToken TMS. В целях усиления безопасности система eToken TMS позволяет использовать дополнительное значение OTP PIN – в этом случае для

аутентификации пользователь помимо имени пользователя и OTP вводит дополнительное секретное значение OTP PIN. Это значение задается при назначении устройства пользователю.

Группа 3. **Специализированные USB-ключи** – представлена одной моделью ключа eToken PRO Anywhere. Электронный USB-ключ eToken Anywhere предоставляет пользователям возможность безопасного доступа к Web-ресурсам с любого компьютера без предварительной установки программного обеспечения. eToken Anywhere обеспечивает:

- Автоматический запуск браузера и направление пользователя только на заранее заданные Web-сайты, адреса которых хранятся в защищённой памяти устройства.
- Аутентификацию пользователя в рамках протокола SSL/TLS и защиту всех данных, передаваемых по сети Интернет.
- Защиту от фишинга и атак типа «человек посередине» (Man in the middle).

Ключ eToken PRO Anywhere сертифицировано ФСТЭК России.

Спецификация eToken PRO Anywhere:

Микросхема смарт-карты: Atmel AT90SC25672RCT

Операционная система смарт-карты: Athena OS755, встроенная виртуальная машина Java (полностью совместимая со стандартом Sun Java Card)

Поддерживаемые интерфейсы и стандарты:

- PKCS#11 версии 2.01,
- Microsoft CryptoAPI,
- PC/SC (команды ADPU),
- Сертификаты X.509 v3, SSL v3, IPSec/IKE.

Аппаратно-реализованные алгоритмы:

- RSA 1024 / 2048,
- DES, 3DES, SHA-1

Объем защищенной памяти 72 КБ на микросхеме смарт-карты.

Поддерживаемые операционные системы:

- **Режим PRO**: Microsoft Windows 2000/2003/XP/Vista/2008/2008 R2/7 (32 и 64-битные версии); Linux; Mac OS,
- **Режим Anywhere**: Microsoft Windows 2003/XP/Vista/2008/2008 R2/7 (32 и 64-битные версии).

Поддерживаемые браузеры Internet Explorer 6.0 и выше, Firefox 3.0 и выше (для режима Anywhere). Поддерживаемые версии драйвера eToken PKI Client 5.1 и выше. Поддерживаемые версии комплекта разработчика: eToken SDK 5.0 и выше. Срок хранения данных в памяти не менее 10 лет. Количество циклов перезаписи памяти не менее 500000.

Назначение комплекса eToken Network Logon

Программно-аппаратный комплекс **eToken Network Logon [6]** – предназначен для кардинального решения проблемы «слабых» паролей при работе на компьютерах под управлением Microsoft Windows. После установки продукта для входа на компьютер или в сеть можно использовать надёжные и стойкие к перебору пароли, либо цифровые сертификаты.

В простейшем сценарии использования eToken Network Logon:

- сгенерирует для пользователя новый сложный пароль для входа в Windows (длиной 14 символов, обязательно содержащий буквы верхнего и нижнего регистра, цифры, спецсимволы);
- сменит текущий пароль пользователя Windows на новый сложный пароль;
- сохранит новый сложный пароль для входа в Windows в защищенной памяти USB-ключа или смарт-карты eToken.

eToken Network Logon обеспечивает:

- Двухфакторную аутентификацию пользователей на компьютере и в сети Windows с помощью USB-ключей или смарт-карт eToken;

- Использование регистрационных имён и паролей для локального входа в систему или для входа в домен;
- Использование цифровых сертификатов X.509, сертификатов пользователя со смарт-картой и закрытых ключей для входа в домен;
- Генерирование и последующее применение случайных паролей, неизвестных пользователю.

eToken Network Logon можно установить на компьютеры и ноутбуки под управлением ОС Microsoft Windows, объединённые в рабочую группу или домен Windows. На компьютере должна быть установлена одна из операционных систем:

- Windows Server 2008 R2;
- Windows Server 2008 (32- или 64-бит);
- Windows Server 2003 R2 (64-бит);
- Windows Server 2003 SP2 (32- или 64-бит);
- Windows 7 (32- или 64-бит);
- Windows Vista SP2 (32- или 64-бит);
- Windows XP SP3 (32-бит);
- Windows XP SP2 (64-бит).

Кроме того, на компьютере должен быть установлен набор драйверов eToken PKI Client 5.1 SP1. Аппаратное обеспечение должно соответствовать требованиям операционной системы. Также необходим свободный USB-порт (при использовании USB-ключей eToken) или устройство чтения смарт-карт (при использовании смарт-карт eToken). eToken Network Logon поддерживает все модели eToken.

После установки eToken Network Logon стандартное приглашение для входа в Microsoft Windows заменяется новым, расширяющим возможности по входу пользователя в систему:

- можно подключить смарт-карту (eToken) с закрытым ключом и сертификатом пользователя, ввести пароль пользователя для eToken и войти в систему;
- можно нажать CTRL+ALT+DELETE, ввести имя пользователя, пароль и (при необходимости) имя домена, нажать OK и войти в систему.

Для каждого из этих двух способов аутентификации в eToken Network Logon предусмотрены усовершенствования:

- Вместо того чтобы каждый раз вводить имя пользователя и сложный пароль, пользователь один раз сохраняет имя в памяти eToken, а впоследствии лишь подключает eToken и вводит для него пароль пользователя.
- Для того чтобы войти в систему, предъявив сертификат пользователя со смарт-картой, надо подключить eToken и ввести для него пароль пользователя. Если eToken уже подключен, не нужно вынимать его и повторно подключать, достаточно лишь нажать CTRL+L, а затем ввести пароль пользователя для eToken.

Установка eToken Network Logon решает проблему "слабых" паролей, так как после установки продукта можно полностью отказаться от использования паролей при входе на компьютер и в сеть, перейдя к использованию цифровых сертификатов, либо использовать хранимые в памяти eToken сложные пароли (заданные вручную с учётом действующих в организации требований к их сложности, либо автоматически сгенерированные). Пароль перестаёт быть "слабым" за счет того, что фактически исключается риск его подбора злоумышленником: при возможной смене пароля пользователем исключается риск задания им нового пароля, являющегося "слабым", пароль не вводится с клавиатуры (исключаются риски подсматривания пароля или его перехвата шпионским ПО), пользователь не должен помнить пароль (исключаются случаи его забывания и записывания на бумаге). С помощью eToken Network Logon можно значительно усилить защищённость существующей системы. Имена и пароли пользователей можно сохранить в памяти eToken, что исключает риск

их подсматривания злоумышленником. Дополнительно можно использовать встроенный в eToken Network Logon генератор паролей для генерации сложных паролей, что уменьшает риск их подбора злоумышленником. Сгенерированный пароль записывается в память eToken и сохраняется в ней. Количество наборов "имя пользователя – пароль", хранящихся в памяти eToken, неограничено параметрами eToken Network Logon и определяется только объемом защищенной памяти используемого устройства.

При развёртывании инфраструктуры PKI (Инфраструктура открытых ключей - Public Key Infrastructure) появляется возможность использовать цифровые сертификаты для входа в сеть Windows и на локальный компьютер. Если в памяти eToken имеется сертификат пользователя со смарт-картой и соответствующий закрытый ключ, их можно использовать для входа в домен Windows вместо имени пользователя и пароля. Таким образом обеспечивается плавность перехода от парольной аутентификации к строгой аутентификации с использованием цифровых сертификатов.

При отсоединении eToken от порта USB происходит автоматическая блокировка компьютера. Для разблокирования компьютера необходимо подсоединить eToken и ввести пароль пользователя для eToken.

Администратор может запретить или разрешить пользователю ввод пароля вручную. Администратор может управлять методами аутентификации, определяя:

- какие методы разрешены на данном компьютере — использование профилей, применение сертификатов;
- какой метод аутентификации используется по умолчанию и может ли пользователь самостоятельно выбирать метод при наличии в памяти eToken как профилей, так и сертификата.

Отметим **основные преимущества eToken Network Logon [7,8,9]**:

- Отказ от ввода паролей вручную — какой бы метод регистрации ни применялся, — использование хранимых в памяти eToken сертификатов или паролей, — при входе в систему пользователь никогда не вводит пароль, что исключает риски подсматривания пароля или его перехвата при вводе с клавиатуры.
- Возможность применения длинных и сложных паролей — поскольку пользователь не должен вводить пароль вручную, сам пароль может быть длиннее и сложнее, чем пользователь может запомнить.
- Использование сгенерированных случайных паролей, неизвестных пользователю — eToken Network Logon позволяет генерировать пароли заданной длины, сохранять их в памяти eToken и подставлять в хранилище учётных данных таким образом, что пользователь даже не знает своего пароля, а потому не может записать и тем самым скомпрометировать пароль.
- Аппаратная аутентификация пользователей — для входа в систему пользователю надо иметь eToken, это более надёжно, чем ввод паролей с клавиатуры.
- Двухфакторная аутентификация — eToken Network Logon позволяет не просто сохранить реквизиты пользователя в памяти eToken, но и защитить их паролем пользователя eToken. При использовании этой возможности потеря или кража eToken не приведёт к компрометации пароля.
- Интеграция в инфраструктуру открытых ключей — eToken Network Logon поддерживает не только системы, в которых для аутентификации пользователей применяются пароли, но и более надёжный и современный метод регистрации с использованием смарт-карт.
- Простота и удобство для пользователей — способы аутентификации, применяемые в eToken Network Logon, удобнее для пользователей, чем

стандартные способы. Требования к сложности паролей пользователя eToken не столь высоки, как требования к сложности паролей Windows. Поэтому при двухфакторной аутентификации вводить простой пароль пользователя eToken проще, чем без таковой вводить сложный и длинный пароль.

- Улучшенный интерфейс при регистрации с использованием смарт-карт — если eToken пользователя подключен к компьютеру, необязательно отключать его и подключать вновь. eToken Network Logon позволяет в таком случае нажать CTRL+L, ввести пароль пользователя eToken и войти в систему, не прикасаясь к eToken.

Отметим также, что eToken Network Logon — универсальный продукт, который можно использовать на изолированном компьютере, в небольшой рабочей группе, в простой или сложной доменной инфраструктуре. Для каждой среды eToken Network Logon позволяет выбрать наилучший с точки зрения безопасности и удобства способ аутентификации. eToken Network Logon можно интегрировать с eToken TMS (Token Management System), системой управления жизненным циклом USB-ключей и смарт-карт, что позволяет управлять сертификатами и профилями централизованно.

Перед выполнением лабораторной работы рекомендуется ознакомиться с информацией по работе с ключами серии eToken, представленной в пособии [10] и электронными ресурсами, доступными в сети Интернет [6,7,8,9].

Практическая часть. Лабораторная работа "*Установка и администрирование eToken Network Logon*"

Цель работы: Знакомство с аппаратными ключами защиты серии eToken. Установка и использование средства защиты eToken Network Logon.

Порядок выполнения практической части лабораторной работы:

1. Установить дистрибутив eToken Network Logon. На компьютер должны быть установлен следующий набор драйверов и дополнительных утилит, обеспечивающих работу с электронными ключами eToken под управлением операционной системы семейства Windows:

    - SafeNet Authentication Client 8.2 для Microsoft Windows 8, Server 2012
    - eToken PKI Client 5.1 SP1 для Microsoft Windows XP, Vista, 7, Server 2003, Server 2008

2. Создать нового пользователя.
3. Подключить eToken с закрытым ключом и сертификатом пользователя, ввести пароль пользователя для eToken и войти в систему;
4. Нажать CTRL+ALT+DELETE, ввести имя пользователя, пароль и (при необходимости) имя домена, нажать OK и войти в систему.

Ход выполнения работы

На рисунке 1 приведено стартовое окно входа после установки дистрибутива eToken Network Logon.

Рисунок 1 – Окно входа

На данном этапе пользователю предлагается ввести пароль от существующей учётной записи или выбрать вариант входа с использованием eToken, а также создать новый профиль (Рисунок 2).

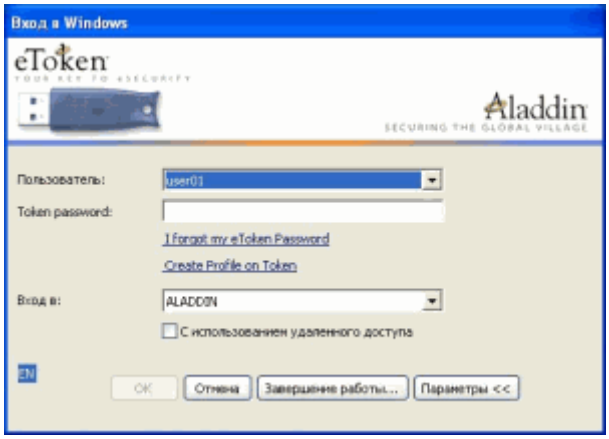

Рисунок 2 – Окно выбора учётной записи пользователя

Окно создание нового профиля показано на Рисунке 3. Режим создания пользователя позволяет использовать существующий пароль для учётной записи или заменить его на новый пароль, созданный пользователем или сгенерированный случайным образом.

Рисунок 3 – Создание нового профиля

После входа в учётную запись для инициализации eToken необходимо запустить eToken PKI Client 5.1. Рабочее окно программы изображено на рисунке 4.

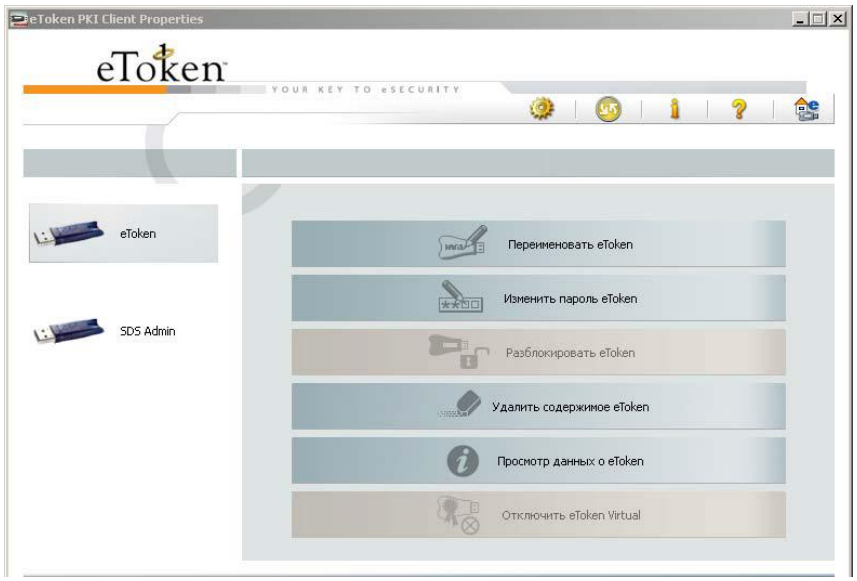

Рисунок 4 – Рабочее окно eToken PKI Client 5.1

На рисунках 5 и 6 изображено меню изменения настроек пароля.

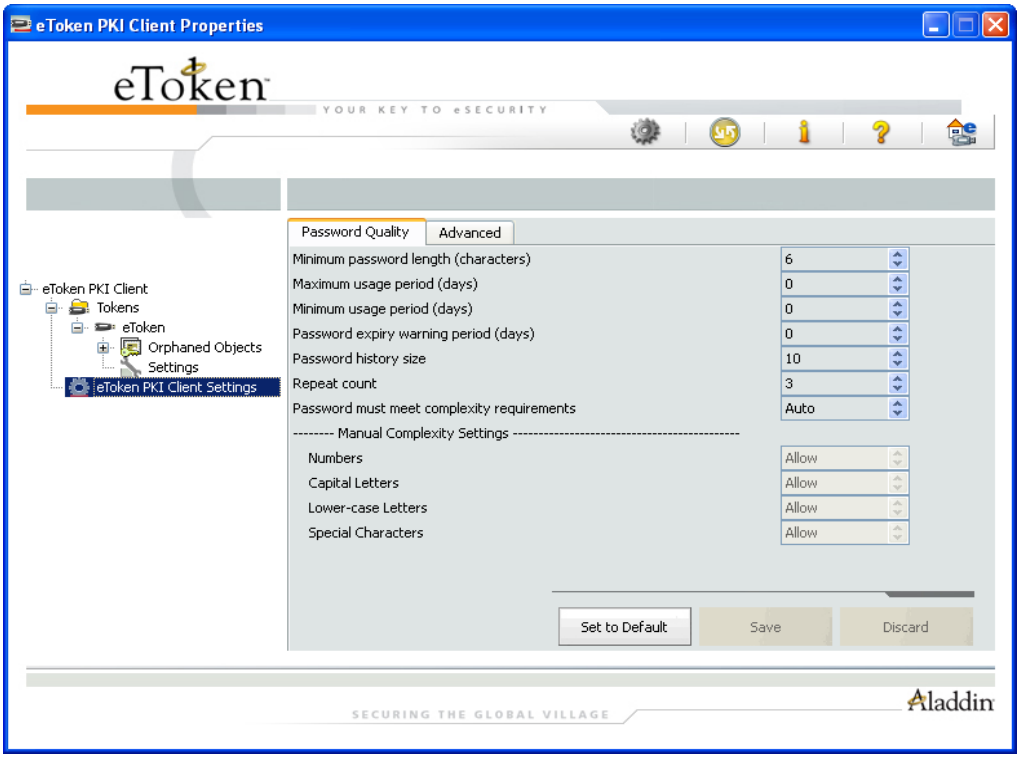

Рисунок 5 – Окно настройки пароля eToken

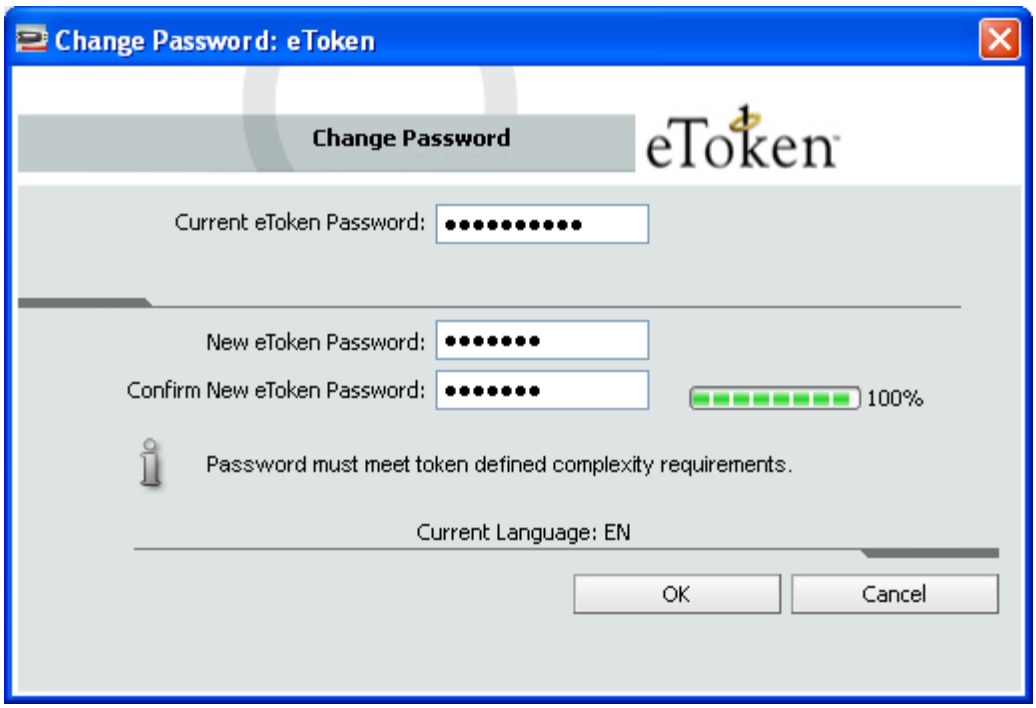

Рисунок 6 – Окно смены пароля eToken

Следующий этап – инициализация eToken. Настройка параметров: *создание пароля пользователя, создание пароля администратора, установка максимально возможных ошибочных вводов пароля*. Процесс инициализации eToken показан на рисунках 7, 8, 9

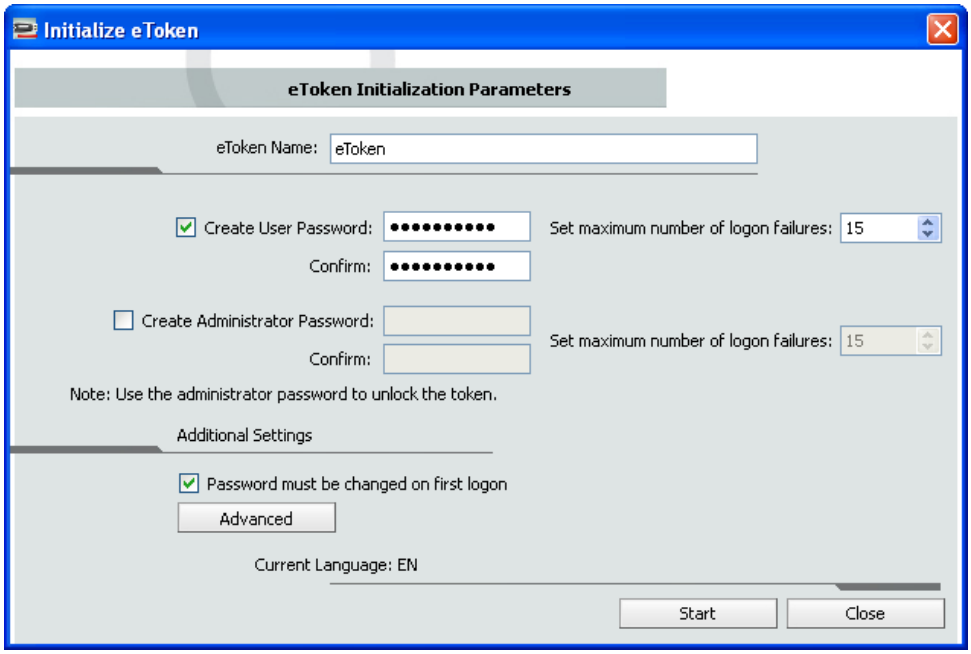

Рисунок 7 – Окно создания паролей eToken

Рисунок 8 – Окно предупреждения

Рисунок 9 – Прогресс инициализации

Требования к содержанию отчета

Отчет выполняется на листах формата А4, которые должны быть скреплены перед сдачей отчета преподавателю. Первый лист отчета титульный – содержит информацию об учебном заведении, кафедре, названии дисциплины, теме выполненной работы. Приводится информация об учащемся, выполнившим работу, информация о преподавателе, проверяющем работу. В нижней части листа информация о месте (городе), где находится учебное заведение и год выполнения работы.

В содержательной части отчета о проделанной работе необходимо указать номер работы и тему работы. Затем описать ход выполнения работы, проиллюстрировать ход выполнения работы скриншотами (копиями экрана), полученными в процессе выполнения работы. Если преподавателем были заданы вопросы по выполнению работы, на которые предложено ответить письменно, то приводятся вопросы и ответы на них. Завершается отчет выводами по проделанной работе. Отмечаются достоинства и недостатки

изученной технологии, область использования разработки и т.д. Желательно привести в отчете список использованной литературы и интернет ресурсов (сайтов сети Интернет).

Контрольные вопросы

1. Назначение комплекса eToken Network Logon, основные характеристики?
2. Решение проблемы "слабых" паролей с помощью eToken Network Logon?
3. USB-ключи серии eToken - eToken ГОСТ, eToken PRO (Java), КриптоПро eToken CSP - основные характеристики, возможность использования с eToken Network Logon?
4. USB-ключи серии eToken - eToken NG-FLASH (Java), eToken NG-OTP (Java) – основные характеристики, возможность использования с eToken Network Logon?
5. Специализированный USB-ключ – eToken PRO Anywhere. Основные характеристики, назначение, возможность использования с eToken Network Logon?
6. Порядок установки и администрирования eToken Network Logon?

Заключение

Выполнение лабораторной работы “Аппаратные ключи eToken. Средство защиты eToken Network logon” позволяет сформировать у учащихся практические навыки по использованию программно-аппаратных схем защиты, которые могут пригодится выпускникам в их производственной деятельности, связанной с проектированием и эксплуатацией защищенных телекоммуникационных систем. Программно-аппаратные средства защиты используются не только для защиты отдельных компьютеров, но и

специализированных устройств, используемых в сетях передачи данных с целью повышения степени защищённости сетей от несанкционированного доступа [11] и, как следствие, надежности сетей передачи данных в целом. С дополнительной информацией по оценке показателей качества обслуживания в мультисервисных сетях можно ознакомиться в [12].

На кафедрах факультета информационных систем и геотехнологий РГГМУ студентам предлагается выполнить цикл лабораторных работ. Пример работы с программно-аппаратными средствами защиты, основанными на использовании ключей серий Hasp (Hasp Hl) и Guardant, приведён в [13].

Теоретические знания и практические умения, полученные в процессе выполнения студентами данной лабораторной работы будут полезны при выполнении других работ, в том числе на учебно-экспериментальном стенде базовой кафедры «Проектирование защищённых телекоммуникационных систем» РГГМУ на предприятии АО «НИИ «Масштаб».

Литература и электронные ресурсы

1. Государственный стандарт РФ ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию».
2. Руководящий документ «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации»
3. Александр Шелупанов, С. Груздев, Ю. Нахаев. Учебное пособие "Аутентификация: от А до Я" [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/support/training/authentication
4. USB-ключи и смарт-карты eToken. [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/catalog/etoken/
5. USB-ключи и смарт-карты eToken – персональное средство аутентификации и защищённого хранения данных. [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/catalog/etoken/models

6. Sentinel HASP — защита, лицензирование и распространение программного обеспечения. [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/catalog/network_logon/
7. Цены и заказ продуктов. [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/buy/?pid=4981
8. USB-ключи и смарт-карты eToken. Официальный прайс-лист. eToken Network Logon [Электронный ресурс] Проверено: 18.05.2015 http://www.aladdin-rd.ru/buy/prices/etoken_user.xls
9. Загрузить главы книги "Аутентификация: теория и практика обеспечения безопасного доступа к информационным ресурсам". [Электронный ресурс] Проверено: 18.05.2015. http://www.aladdin-rd.ru/upload/Authentication_Book.zip
10. Шелупанов А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. / А. Шелупанов, С. Груздев, Ю. Нахаев, 552 стр., Издательство: Горячая Линия – Телеком, 2009г.
11. Шапаренко Ю.М., Бескид П.П., Суходольский В.Ю. Проектирование защищённых информационных систем. Часть1.Конструкторское проектирование. Защита от физических полей. (учебное пособие). СПб: Изд-во РГГМУ, 2008г. с. 60
12. Смирнов П.И. Способы оценки показателей качества обслуживания в мультисервисных сетях. Журнал «Вопросы радиоэлектроники». Сер. «СОИУ». Вып.2. – М: ОАО «ЦНИИ «Электроника», 2012. с.51-63
13. Ананченко И.В., Мусаев А.А. Защита приложений, выполняемых торговым терминалом Metatrader, ключами Sentinel HASP. Труды СПИИРАН. 2013. № 3 (26). с. 69-78.

ОГЛАВЛЕНИЕ

Ананченко Игорь Викторович
Смирнов Павел Игоревич
Шапаренко Юрий Михайлович

АППАРАТНЫЕ КЛЮЧИ ETOKEN. СРЕДСТВО ЗАЩИТЫ ETOKEN NETWORK LOGON

Методические указания

Редактор И.Г. Максимова

Подписано в печать Формат 60/901/2 Бумага книжно – журнальная
Печ. л. Тир. 55
РГГМУ, 195196, СПб, Малоохтинский пр., Отпечатано