

Лабораторная работа 6. Аутентификация в операционных системах при помощи физического объекта

Цель лабораторной работы: рассмотреть утилиты и приложения, позволяющие производить аутентификацию в операционной системе (ОС) при помощи физического объекта – eToken.

Задачи лабораторной работы:

1. Базовые действия с eToken
2. Установка требований к качеству PIN-кода eToken
3. Администрирование eToken
4. Аутентификация в ОС при помощи eToken
5. Аутентификация в ОС на основе случайного пароля
6. Администрирование eTokenNetworkLogon

Задание

Контрольные вопросы

Содержание лабораторной работы:

В лабораторной работе пароль для входа в операционную систему хранится на физическом объекте, а для доступа к нему используется PIN-код на eToken. Для подключения eToken к компьютеру используется USB-порт.

Рассматриваемые утилиты и приложения:

- *утилита управления eToken - позволяет устанавливать качество PIN-кода к нему;*
- *eToken Network Logon - позволяет использовать eToken для хранения аутентификационных данных для входа в ОС.*

1. Базовые действия с eToken

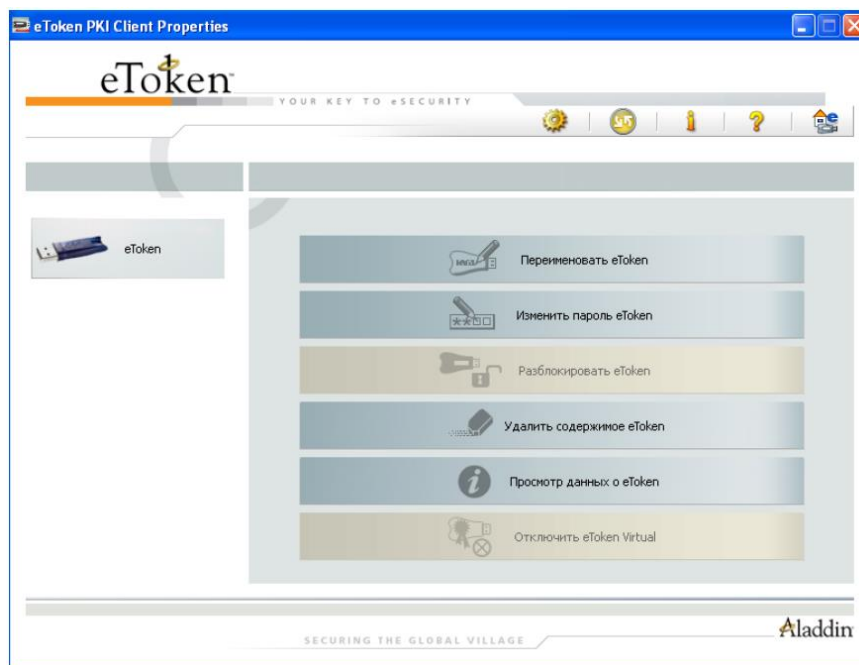


Рис. 1 - Вид основного окна утилиты «eToken Properties»

Запустите виртуальную ОС и войдите под учётной записью «Администратор». Подключите eToken к USB-порту. Запустите утилиту «eToken Properties»: «Пуск - Программы - eToken - eToken Properties» (или через значок «eToken PKI Client» на панели уведомлений). Вид основного окна представлен на рис. 1.

Смените PIN-код. Используемый по умолчанию PIN-код: «1234567890». При смене PIN-кода необходимо соблюдать требования, предъявляемые к его качеству. Достижение отметки 100% означает, что введенный PIN-код отвечает установленным требованиям (рис. 2).

Рис. 2 - Смена PIN-кода

Переименуйте eToken (рис. 3). Для возможности простого определения принадлежности eToken необходимо присвоить ему уникальный в системе идентификатор пользователя (login), которому выдаётся eToken. При первой операции с eToken необходимо ввести PIN-код.

Измените режим интерфейса на «Подробный вид» (значок на панели инструментов). В данном режиме предоставляется доступ к дополнительным настройкам и функциям по работе с подключенными eToken (рис. 4). В основном окне режима «Подробный вид» предоставляется информация о выбранном eToken.

Рис. 3 - Переименование eToken

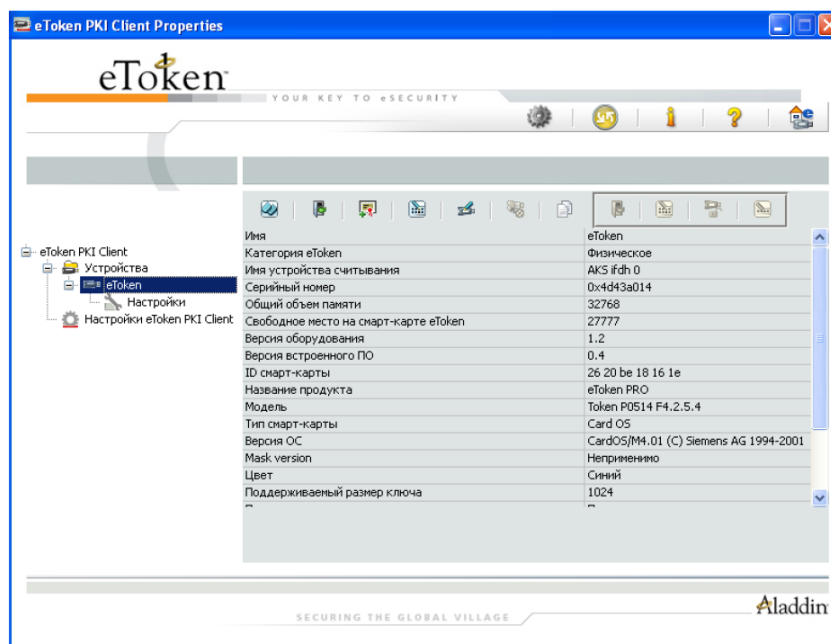


Рис. 4 - Вид основного окна для eToken в режиме «Подробный вид»

2. Установка требований к качеству PIN-кода eToken

В разделе «Настройки eToken PKI Client» возможна установка требований к качеству PIN-кода eToken, которые будут записаны на него при форматировании (рис. 5). Просмотр требований, сохранённых на eToken, возможен в разделе «Настройки» выбранного eToken.

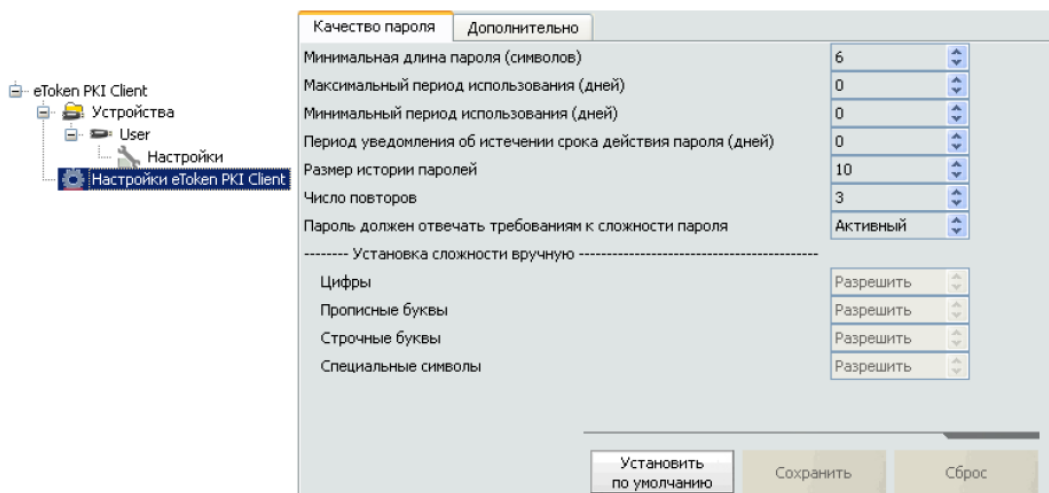


Рис. 5 - Настройка параметров качества PIN-кода eToken

3. Администрирование eToken

В режиме «Подробный вид» выберите подключенный eToken и на панели инструментов выберите «Инициализировать eToken». В окне «Параметры инициализации eToken» (рис. 6) установите PIN-код eToken или требование к обязательной смене пароля при первом использовании (если оставите PIN-код по умолчанию), а также PIN-код администратора eToken. Также можно установить максимальное количество ошибок ввода соответствующих PIN-кодов и имя eToken. Отформатируйте eToken. **Внимание!** При форматировании есть возможность указать ключ форматирования («Дополнительно» - «Изменить ключ инициализации»). **Не изменяйте** настройки этой вкладки, так как при

незнании ключа форматирования нельзя восстановить его в первоначальном состоянии, что приводит к неработоспособности eToken.

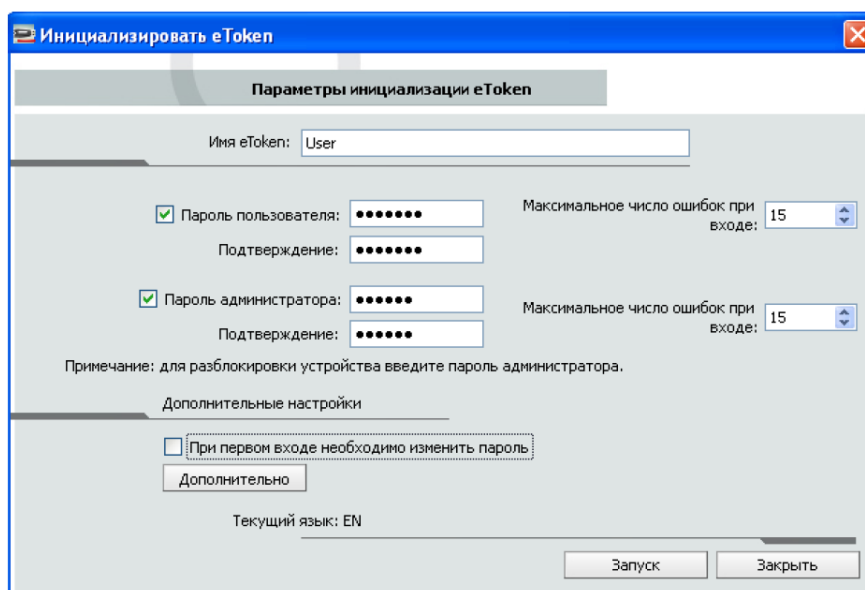


Рис. 6 - Параметры инициализации eToken

Выберите подключенный eToken. На панели инструментов выберите значок «Вход с правами администратора». Введите PIN-код администратора (рис. 7). Администратору предоставляются дополнительные функции. На панели инструментов выберите значок «Установить пароль пользователя». Эта функция позволяет администратору задать новый PIN-код eToken, если пользователь забыл свой текущий PIN-код.

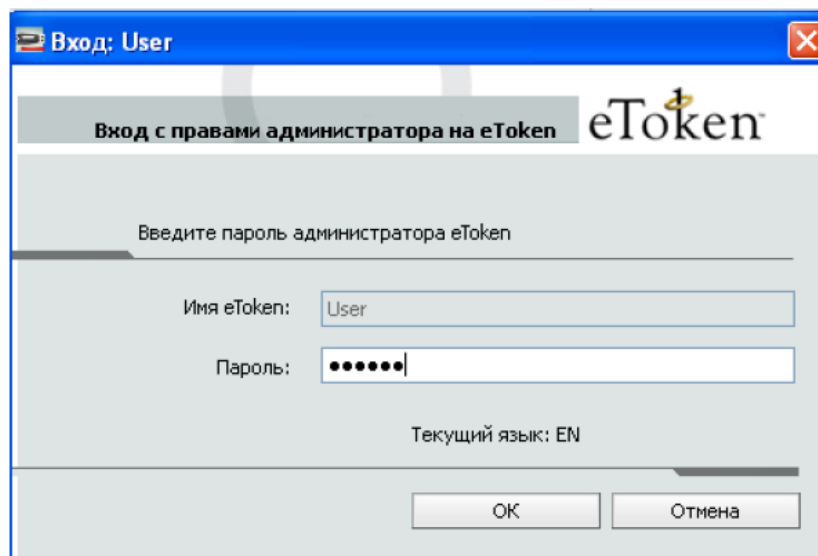


Рис. 7 - Ввод пароля администратора

Настройки интерфейса утилиты «Свойства eToken» можно изменять через «Групповые политики», используя соответствующий административный шаблон. Откройте оснастку gpedit.msc и добавьте административный шаблон eTokenPKIClient.adm (расположен на «Рабочем столе»). В появившемся разделе «eToken PKI Client Settings» можно разрешать или запрещать доступ к любой настройке рассматриваемой утилиты. Например, запретите доступ к режиму «Подробный вид» (значение 0 настройки «OpenAdvancedView» параметра «Access Control» раздела «UI Access Control List», рис. 8). Для проверки внесённых изменений перезапустите утилиту «Свойства eToken».

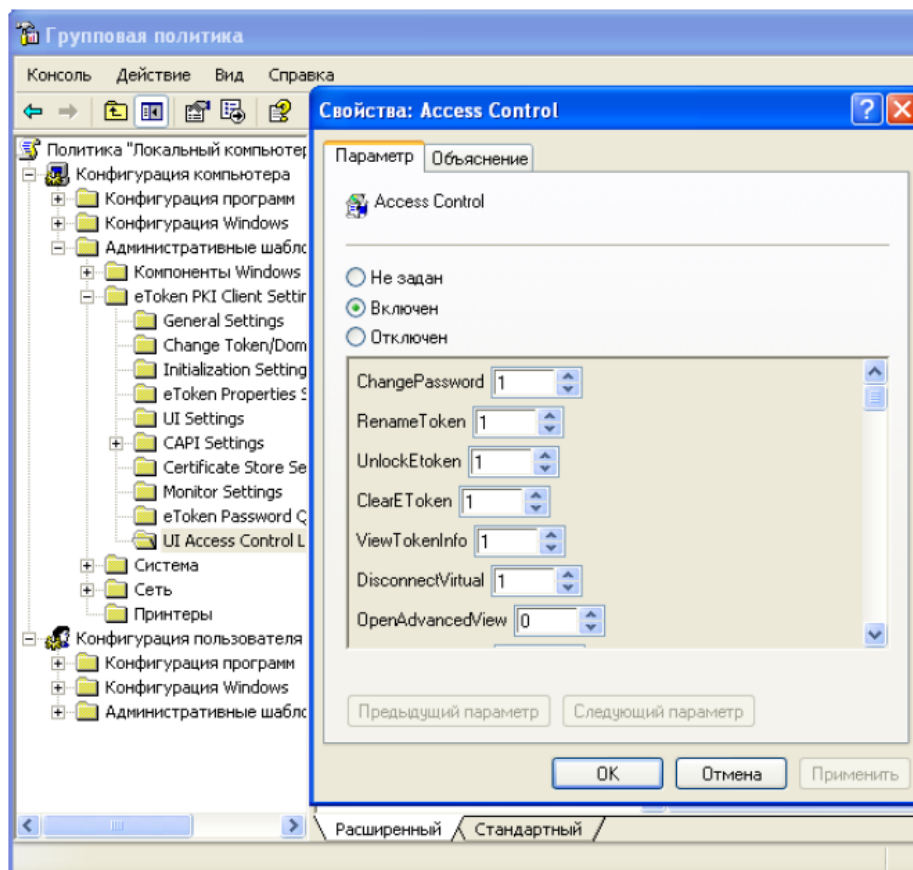


Рис. 8 - Запрет доступа к режиму «Дополнительно»

4. Аутентификация в ОС при помощи eToken

Запустите утилиту для создания профиля входа в операционную систему: «Пуск - Программы - eToken - eToken Network Logon - eToken Network Logon Profile Wizard». Нажмите «Далее». Введите логин пользователя (например, «User») и название рабочей станции (либо домена), для которых создаётся профиль (рис. 9). Нажмите «Далее».



Рис. 9 - Ввод информации пользователя для входа в ОС

Введите и подтвердите пароль для входа в ОС, принадлежащий выбранному пользователю (рис. 10). Дважды нажмите «Далее». Введите PIN-код eToken для подтверждения записи на него созданного профиля.



Рис. 10 - Ввод пароля для входа в ОС

Завершите текущий сеанс пользователя и отключите eToken. При появлении «окна приветствия» Windows подключите eToken. Появится окно, изображённое на рис. 11. Введите PIN-код eToken и нажмите кнопку «ОК». С eToken будет считана необходимая аутентификационная информация и произведён вход в ОС. После входа в ОС отключите eToken - в этом случае сеанс пользователя блокируется. Подключите eToken и разблокируйте сеанс.

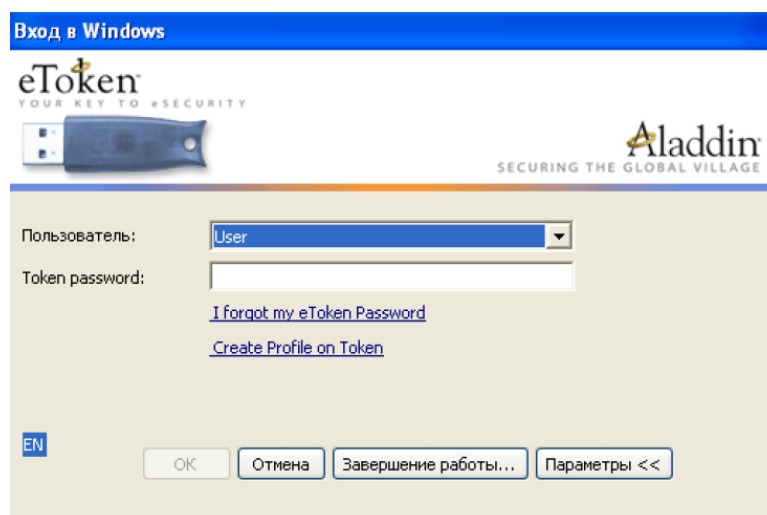


Рис. 11 - Двухфакторная аутентификация при помощи eToken

Сменить пароль для входа в ОС можно, используя встроенные в ОС средства. Нажмите Ctrl-Alt-Del и выберите «Смена пароля...». В появившемся окне (рис. 12), кроме нового пароля и его подтверждения необходимо ввести PIN-код eToken для записи на него нового пароля.

Рис. 12 - Смена пароля для входа в ОС

Сменить пароль также можно при помощи утилиты «eToken Network Logon Profile Wizard». В окне (рис. 13) выберите существующий на eToken профиль. В окне (рис. 14) выберите создание нового пароля и включите параметр обновления пароля в хранилище ОС («Update domain password in directory»). Введите текущий и новый пароли. Если текущий пароль уже есть на eToken, то включите параметр «Read current domain password from eToken» и утилита автоматически считывает его из существующего профиля.

Рис. 13 - Выбор существующего на eToken профиля

Рис. 14 - Смена пароля для входа в ОС

Для удаления, существующего на eToken профиля нужно в окне (рис.15) выбрать «Remove an existing profile». Удалите существующий профиль.



Рис. 15 - Выбор двухфакторной аутентификации

5. Аутентификация в ОС на основе случайного пароля

Создайте новый профиль для входа в ОС, выбрав задание случайного пароля определённой длины (рис. 16). Тогда пароль для входа в ОС будет храниться только на eToken, иметь высокую сложность, не будет известен пользователю, уменьшая возможность подбора или разглашения пароля. После создания профиля завершите сеанс пользователя. Отключите eToken. При попытке стандартного входа в ОС (через Ctrl-Alt-Del) старый пароль пользователя будет отклонён, т.к. произошла смена пароля на случайный с заданной длиной. Войдите в ОС с использованием eToken.

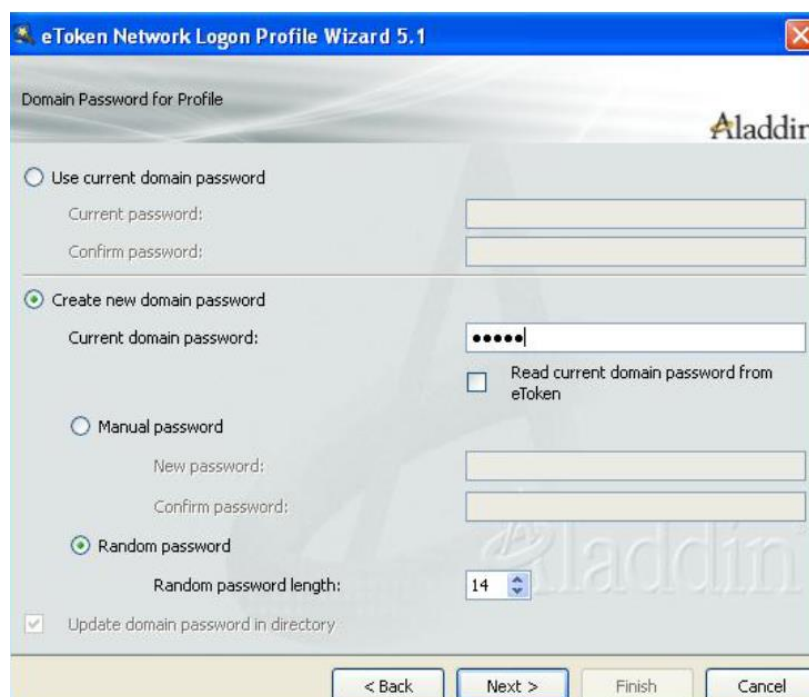


Рис. 16 - Задание случайного пароля для входа в ОС

Сменить случайный пароль для входа в ОС пользователь может, выбрав «Смена пароля...» при нажатии Ctrl-Alt-Del (рис. 17). В этом случае достаточно ввести PIN-код eToken, а новый пароль для входа в ОС будет сгенерирован случайным образом. Длина случайного пароля будет задана в соответствии с настройками.

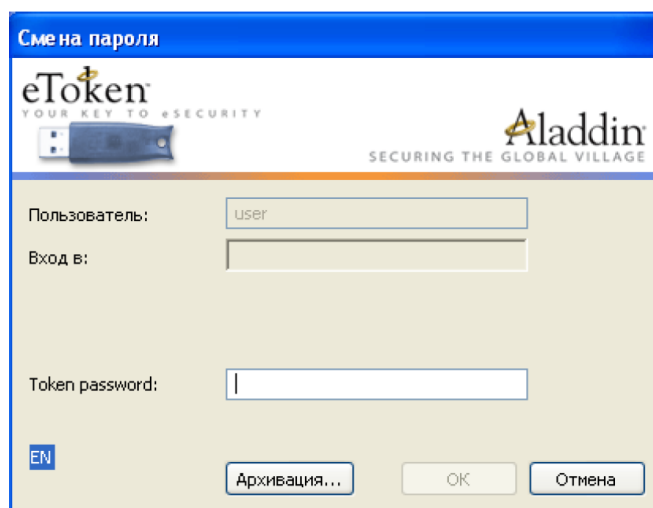


Рис. 17 - Смена случайно заданного пароля для входа в ОС

6. Администрирование eTokenNetworkLogon

Настройки рассматриваемой утилиты можно изменять через «Групповые политики», используя соответствующий административный шаблон. Под учётной записью «Администратор» откройте gpedit.msc, добавьте административный шаблон «C:\Program Files\Aladdin\eToken\eTNLogon\eTokenNetworkLogon.adm». В разделе «eTokenNetworkLogon» можно разрешать или запрещать доступ к любой настройке, а также включать и отключать функции рассматриваемой утилиты. Например, запретите стандартный вход в ОС через Ctrl-Alt-Del (значение 0 параметра «Allow Standard Windows Logon») - будет разрешён вход только с использованием eToken (рис. 18). Завершите сеанс пользователя. Попробуйте воспользоваться стандартным методом входа в ОС.

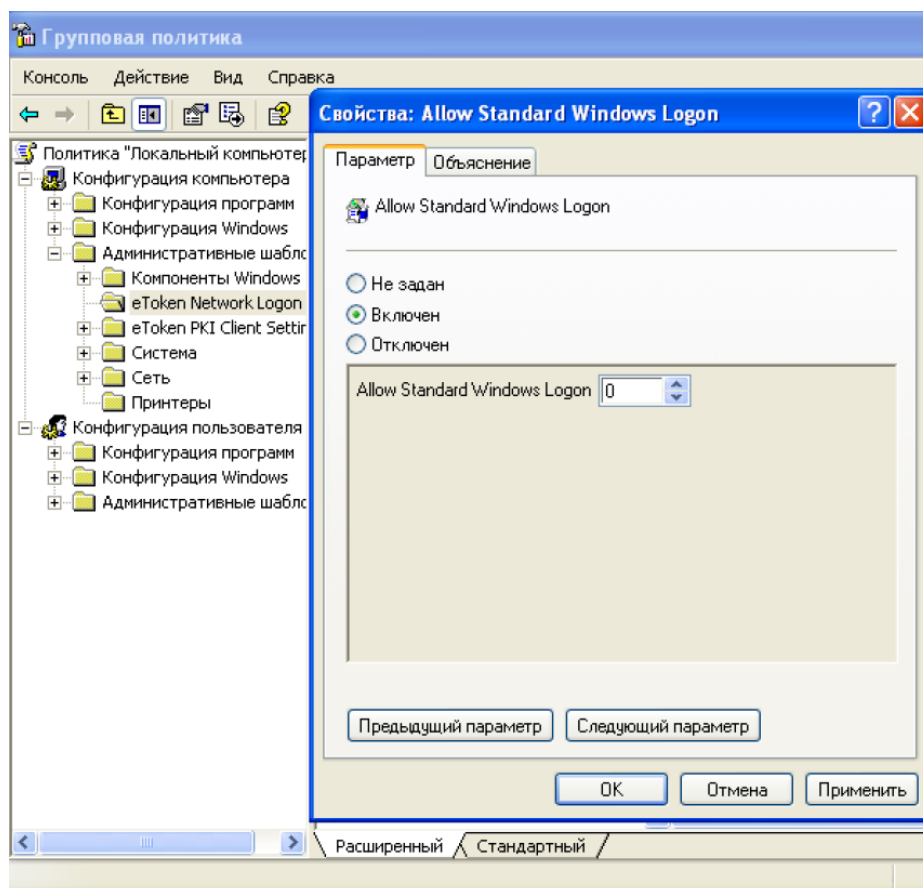


Рис. 18 - Запрет стандартного входа в ОС

Для входа с правами администратора создайте для учётной записи «Администратор» новый профиль на eToken при помощи функции «Create profile on Token» (рис. 19).

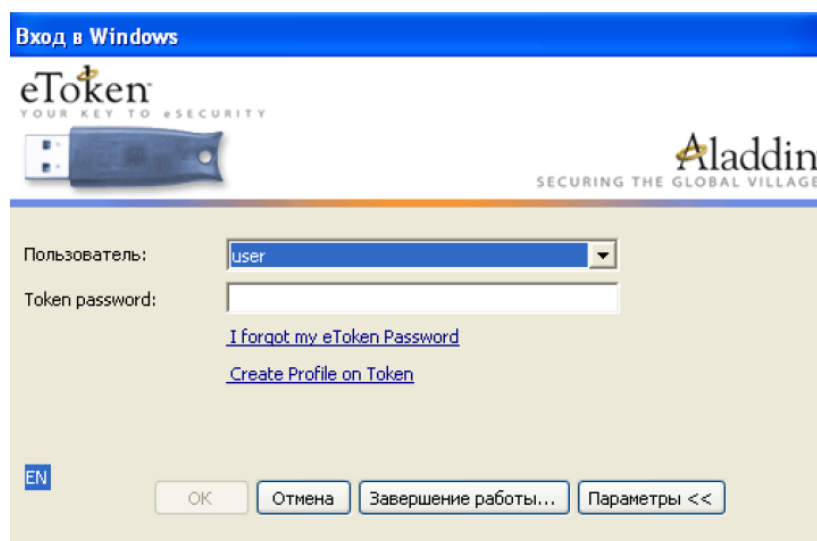


Рис. 19 - Функции по работе с eToken, доступные до входа в ОС

Задание

1. Создайте пользователя с именем, совпадающим с Вашим именем в кафедральной сети.
2. Установите требования к качеству PIN-кода eToken в соответствии с Вашим вариантом (табл. 1).
3. Отформатируйте eToken, присвоив ему имя созданного пользователя и установив пароль, соответствующий требованиям п. 2.
4. Создайте профиль для входа в ОС созданного пользователя.
5. Прдемонстрируйте преподавателю процедуру смены пароля для входа в ОС в соответствии с параметрами, указанными в Вашем варианте.

Таблица 1. Варианты заданий

Вар.	Требования к качеству PIN-кода	Параметры входа в ОС
1	Мин. длина пароля - 8 символов. Макс. срок действия пароля - 30 дней.	Ввод нового пароля вручную. Ввод текущего пароля вручную.
2	Мин. длина пароля - 12 символов. Количество хранимых последних паролей - 5.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
3	Мин. длина пароля - 12 символов. Пароль должен содержать только буквы обоих регистров.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
4	Макс. срок действия пароля - 30 дней. Пароль должен содержать все типы символов.	Генерация случайного нового пароля длиной 10 символов. Ввод текущего пароля вручную.
5	Макс. срок действия пароля - 40 дней. Количество хранимых последних паролей - 8.	Генерация случайного нового пароля длиной 10 символов. Считывание текущего пароля с eToken.
6	Мин. длина пароля - 10 символов. Пароль должен содержать только буквы обоих	Генерация случайного нового пароля длиной 10 символов.

	регистров и числа.	Ввод текущего пароля вручную.
7	Мин. длина пароля - 12 символов. Пароль может содержать все типы символов.	Генерация случайного нового пароля длиной 15 символов. Ввод текущего пароля вручную.
8	Макс. срок действия пароля - 30 дней. За сколько дней пользователь должен быть предупреждён о смене пароля - 3 дня.	Генерация случайного нового пароля длиной 15 символов. Считывание текущего пароля с eToken.
9	Количество хранимых последних паролей - 7. Пароль должен содержать только буквы обоих регистров и числа.	Изменение пароля через Ctrl-Alt-Del.
10	Количество хранимых последних паролей - 9. Пароль должен содержать все типы символов.	Изменение случайно заданного пароля через Ctrl- Alt-Del.

Контрольные вопросы

1. Какой PIN-код для eToken используется по умолчанию?
2. Каким образом можно узнать размер свободной памяти на eToken?
3. Какие дополнительные возможности предоставляются администратору eToken?
4. Какие можно установить требования к качеству PIN-кода eToken?
5. Где хранятся требования к качеству PIN-кода eToken, используемые при смене этого PIN-кода?
6. Опишите отличия двухфакторной аутентификации при использовании eToken от однофакторной.
7. Что включает профиль входа в операционную систему, создаваемый приложением eToken Network Logon?
8. С использованием каких способов может происходить смена пользователем пароля на вход в операционную систему?
9. Каким образом происходит смена пользователем случайно установленного пароля для входа в операционную систему?
10. Каким образом настраивается доступность для пользователя различных функций eToken Properties и eToken Network Logon?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях