

**АУТЕНТИФИКАЦИЯ В WINDOWS®
И В ПРИЛОЖЕНИЯХ**
с использованием электронных ключей

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

© ISBC
Москва, 2006

Настоящее "Руководство пользователя" является частью программно-аппаратного комплекса ESMART® Access, предназначено для его пользователей, и содержит сведения о продукте и его применении.

Компания **"Интеллектуальные системы управления бизнесом"** не несет ответственности за технические или редакторские ошибки или опечатки, возможные в данном руководстве, а так же за случайные или непреднамеренные повреждения, вызванные использованием этого материала или продукта.

Компания **"Интеллектуальные системы управления бизнесом"** не несет ответственности за повреждения иной собственности из-за любых дефектов продукта, за прямые или косвенные потери, возникшие в результате использования или неиспользования продукта.

Авторские права на "Руководство пользователя" принадлежат компании ООО **"Интеллектуальные системы управления бизнесом"**.

Содержание данного "Руководства пользователя" не может быть переведено или издано в любой форме, электронной или механической, включая фотокопию, репринтное воспроизведение, запись или использование в любой информационной системе, без получения разрешения компании ООО **"Интеллектуальные системы управления бизнесом"**.

Встречающиеся в данном документе наименования и словосочетания могут являться зарегистрированными торговыми знаками или другими зарегистрированными правами соответствующих фирм.

Содержание

Раздел 1. Программно-аппаратный комплекс ESMART® Access	4
О системе ESMART® Access	4
Системные требования	5
Раздел 2. Установка программно-аппаратного комплекса.....	5
Часть 1. Установка аппаратной части.....	5
Часть 2. Установка программной части	7
Архитектура системы.....	10
Раздел 3. Активация ESMART® Access	11
Раздел 4. Работа с программой ESMART® Access : Administrator.....	12
Общие принципы работы с программой	12
Настройки	13
Вход в Windows.....	13
Менеджер паролей	14
Электронный ключ.....	15
ЭК: при вставлении.....	16
ЭК: при извлечении	17
Язык.....	17
Разметка электронных ключей.....	18
Создание учетных записей.....	21
Редактирование учетных записей.....	23
Удаление учетных записей.....	24
Автоматический выбор учетной записи.....	24
Менеджер паролей	24
Редактирование парольных записей.....	25
Создание и редактирование шаблонов.....	28
Экспорт и импорт шаблонов	29
Редактирование парольных записей WEB.....	30
Программа ESMART® Access: Trau. Применение парольных записей	31
Редактирование записной книжки	33
Резервное копирование.....	33
Операции с ключами доступа	34
Смена владельца электронного ключа	35
Просмотр текущей разметки ключа	35
Работа с модулем входа в систему ESMART® Access : GINA.....	35
Регистрация в системе	35
Действия пользователя после входа в систему.....	37
Состояние блокировки компьютера	38
Раздел 5. Особенности различных электронных ключей	39
1. ESMART® Access card.....	39
2. Карты Schlumberger Cryptoflex.....	39
3. Aladdin eToken PRO	40
4. USB drive.....	40
5. Карты ESMART® Access Lite	40
Раздел 6. Удаление ESMART® Access	41

Раздел 1. Программно-аппаратный комплекс ESMART® Access

О системе ESMART® Access

Система ESMART® Access (EA) представляет собой программно-аппаратный комплекс. Основное назначение состоит в безопасном хранении учетных записей пользователей на аппаратных устройствах защищенной памяти (электронных ключах) для последующего их использования при входе в Windows® NT – совместимые системы, в пользовательских приложениях и WEB-сайтах.

Комплекс предназначен для пользователей, обладающих навыками работы на IBM-совместимых Персональных Компьютерах с операционной системой Windows® и изучившими настоящее руководство пользователя.

Программная часть состоит из следующих компонент:

1. ESMART® Access : GINA – компонента, обеспечивающая вход пользователей в операционную систему с использованием электронных ключей
2. ESMART® Access : Administrator - компонента для редактирования содержимого электронных ключей и управления настройками системы;
3. ESMART® Access : Tray – компонента, в задачи которой входит реализация функций менеджера паролей. Визуально выполнена в виде иконки, которая расположена в области уведомлений Windows®.
4. ESMART® Access : IE Extension – компонента для поддержки функции менеджера паролей в WEB формах браузера Internet Explorer.
5. Модули поддержки отдельных типов электронных ключей (токен-модули).

Все программы обладают интуитивно понятным пользовательским интерфейсом. С технической точки зрения, система построена по модульному принципу, что позволяет использовать в системе самые различные электронные ключи – от смарт карт до широко распространенных устройств flash памяти.

Продукт нацелен на самый широкий спектр пользователей – от домашних до корпоративных. При использовании определенных типов электронных ключей достигается совместимость с инфраструктурой PKI. Это открывает широкие возможности для применения электронных ключей в составе таких приложений, как безопасная электронная почта (secure email).

Аппаратная часть системы может варьироваться в зависимости от потребностей и предпочтений заказчика. Возможны следующие варианты:

- Считыватель смарт-карт + карты. Возможен выбор типа карт в зависимости от требований;
- USB токены (подключаются напрямую в USB порт, не требуют считывателя);
- USB flash drive (подключается напрямую в USB порт, не требует считывателя).

Системные требования

Персональный компьютер (минимальная конфигурация):

- Процессор: Intel Pentium 133 MHz (или аналогичный) и выше;
- Оперативная память: 32 Mb для MS Windows® 2000, 128 Mb для MS Windows® XP/2003;
- Свободное пространство на жестком диске: 15 Mb;
- Монитор с разрешением экрана не менее 800x600 (рекомендуется 1024x768 и выше);
- CD-ROM;
- Мышь или аналогичное устройство;
- Свободный USB или COM порт.

Программное обеспечение:

- Операционная система (ОС): MS Windows® 2000 (требуется Service Pack 4), XP, 2003.




Раздел 2. Установка программно-аппаратного комплекса

Часть 1. Установка аппаратной части

В качестве считывателя смарт-карт **обычно** используются изделия на базе чипсета ACR30 производства фирмы "Advanced Card Systems" или CardMan фирмы OMNIKEY. Включенные в комплекс считыватели серийно выпускаются фирмой для работы со смарт-картами на персональном компьютере через последовательный (COM / USB) порт.

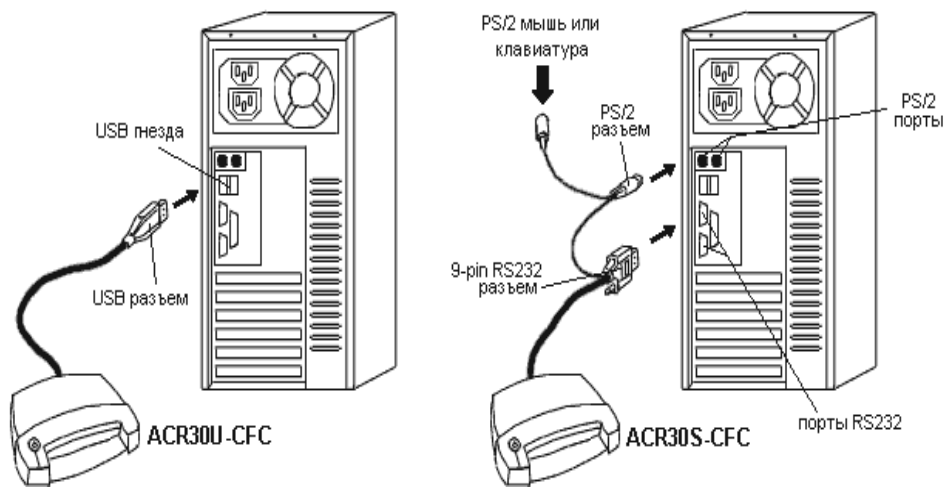
В комплектацию ESMART® Access могут входить считыватели следующих типов:

Табл. 1

Наименование / Внешний вид		Описание
	OMNIKEY CardMan 3121 Цвет корпуса черный с серым. Интерфейс USB 2.0.	Компактный внешний считыватель смарт-карт, поддерживающее все микропроцессорные смарт-карты с протоколами T=0 и T=1, а также карты памяти всех известных производителей.
	ACR30U(S)-PNC Корпус из белого пластика выполненный в виде "пианино" (piano case)	
	ACR30S(U)-CFC Корпус из серого или синего прозрачного пластика выполненного в виде "лягушки" (cyberfrog case)	

	<p align="center">ACR38U-SPC</p> <p>Корпус из серого металлизированного пластика с темной полупрозрачной вставкой, выполненный в "космическом" стиле (space case)</p>	
<p>ACK30S(U)-S</p> 	<p>Считыватель смарт-карт интегрирован в мультимедийную клавиатуру.</p>	
<p>ACF30U(S)-S1(4)S</p> 	<p>Пластмассовый корпус, соответствующий размерам стандартного 3.5" Floppy дисковод, позволяет встраивать считыватель внутрь корпуса компьютера в 3,5" или 5" дюймовый отсек. Считыватель использует внутреннее питание компьютера.</p>	



Подключение считывателей смарт-карт





Для подключения USB-считывателя нужно вставить разъем его шнура в свободный USB порт компьютера или USB хаба. Для подключения COM - считывателя нужно вставить его в разъем клавиатуры или мыши и в COM-порт.

Подключение USB drive и USB-ключей Aladdin eToken

USB flash накопитель (USB-drive)	USB-ключ
	Aladdin – eToken PRO
	

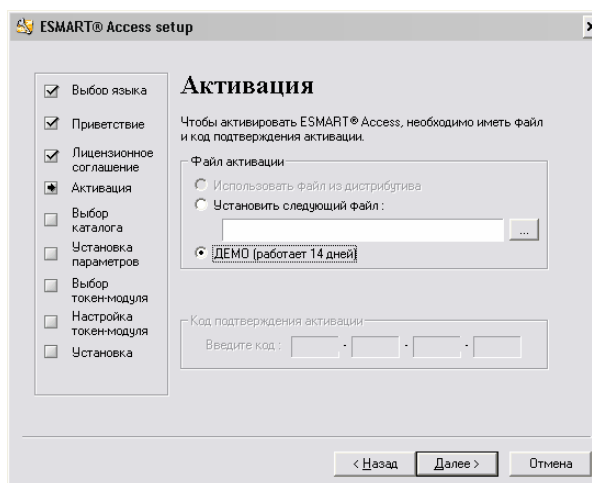
Устройства подключаются напрямую в USB порт компьютера. Однако, прямое подключение к задней стенке компьютера крайне неудобно. Если корпус компьютера не оборудован фронтальными USB разъемами, рекомендуется использовать кабели-удлинители.

Часть 2. Установка программной части

Чтобы начать установку запустите исполняемый файл *setup.exe* из дистрибутива ESMART® Access. Процесс установки разделен на шаги, предельно прост и понятен. Следуйте указаниям мастера. Обратим внимание на следующее:

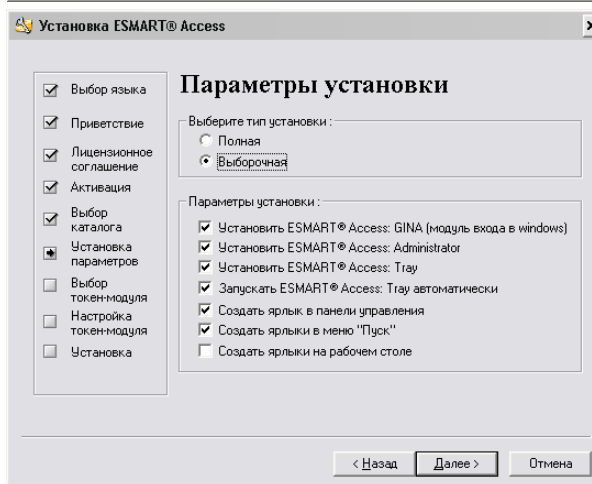
Для активации продукта необходим файл и код подтверждения активации. Их можно получить в процессе регистрации программного продукта, который подробно описан в настоящем руководстве.

Без активации программа работает 14 дней. После прошествия 14 дней работа с электронными ключами становится невозможной. Вы должны или зарегистрировать программу, или удалить ее из системы. Если у Вас на момент установки уже есть файл и код подтверждения активации, Вы можете зарегистрировать Вашу копию прямо в программе установки.



Установка ESMART® Access : GINA необходима, если Вы планируете на этом компьютере регистрироваться в операционной системе посредством электронных ключей. После перезагрузки у Вас поменяется интерфейс входа в Windows®.

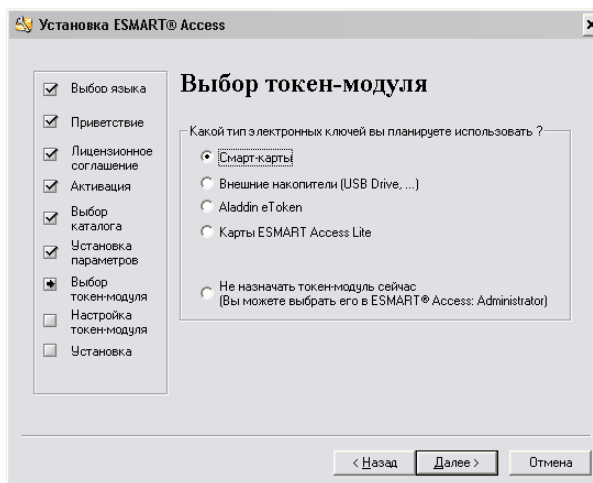
Если на компьютере необходимо персонализировать карты, прописывать на них учетные записи, создавать и редактировать парольные записи, или же Вы хотите пользоваться записной книжкой, то нужно устанавливать программу ESMART® Access : Administrator.



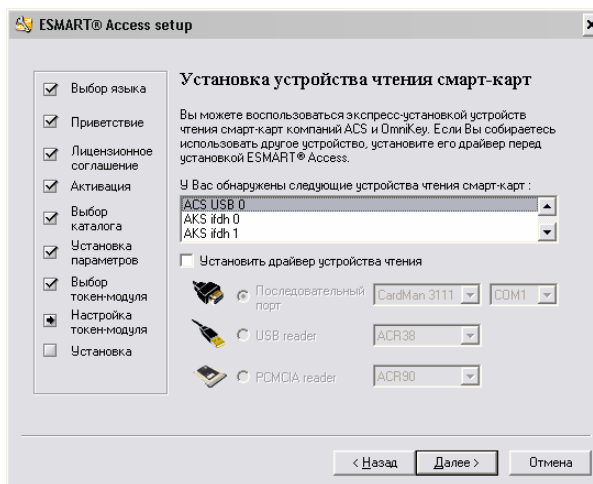
Если Вы хотите, чтобы ESMART® Access : Administrator можно было запускать не только из меню "Пуск", но так же из панели управления, то пометьте соответствующий флажок.

ESMART® Access : Tray внешне выглядит в виде значка в правом нижнем углу рабочего стола. Она позволяет применять к окнам и WEB сайтам ранее созданные и сохраненные в электронный ключ парольные записи. Если Вам не нужно вставлять пароли в пользовательские приложения, то мы рекомендуем исключить ESMART® Access : Tray из автозапуска или не устанавливать его в целях экономии ресурсов компьютера.

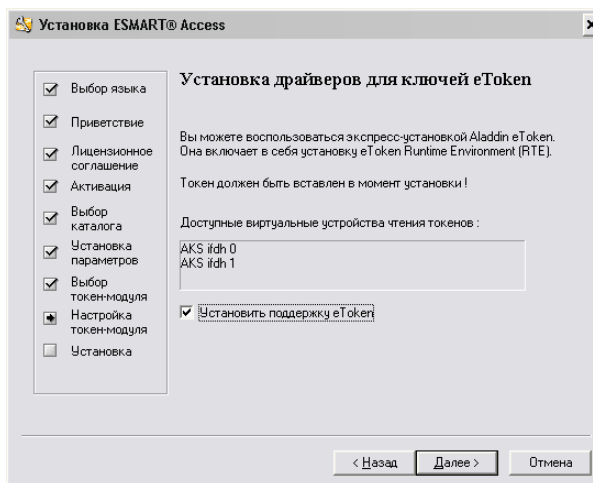
В процессе установки можно выбрать токен-модуль, с которым вы будете работать. Он будет автоматически подключен к системе. Если программа устанавливалась ранее, и Вы выбираете “не назначать токен-модуль сейчас”, то текущая настройка не будет изменена. Если программа ранее не устанавливалась, то система будет работать без поддержки электронных ключей.



Если Вы выбрали работу со смарт-картами, установщик может настроить драйверы считывателей смарт-карт компаний Advanced Card Systems и OmniKey. **Считыватель должен быть подключен к компьютеру перед началом установки!**



Если Вы выбрали работу с Aladdin eToken, установщик предложит Вам установить компоненты, необходимые для работы этих устройств. Работа с eToken осуществляется через виртуальный считыватель смарт-карт.



Архитектура системы

Архитектура системы ESMART® Access представляет собой абстрактную аппаратно-независимую модель. Особенности тех или иных электронных ключей скрыты внутри токен модулей и в большинстве случаев никак не отражаются на действиях пользователя.

Электронный ключ рассматривается как устройство памяти, поддерживающее функции контроля доступа к хранимой на нем информации. Функции контроля доступа должны удовлетворять требованиям модели безопасности, о которых будет рассказано ниже. Если устройство не поддерживает функции контроля доступа, то они реализуются программной эмуляцией внутри токеномодуля. В последнем случае фактическая безопасность является однофакторной, то есть базируется лишь на том, что пользователи “имеет”, а именно сам электронный ключ. При утере электронного ключа информация на нем может быть расшифрована после изучения алгоритмов шифрования, реализованных в токеномодуле. Хотя реверсирование алгоритмов и требует высокой квалификации, но не содержит в себе ничего принципиально невозможного. Перед использованием устройств, не поддерживающих аппаратную защиту информации, вы должны оценить все риски, с этим связанные. К таким устройствами относятся USB flash drive и карты памяти (ESMART® Access Card Lite). Все смарт-карты и USB ключи поддерживают двухфакторную аутентификацию, основанную на том, что пользователь “имеет” и что он “знает”.

Защита хранимой в электронном ключе информации основана на двух секретных кодах длиной от 0 до 8 символов:

- Мастер код (МК);
- ПИН код (PIN).

Предполагается, что пользователи разделены на 2 категории: администраторы и обычные пользователи. В задачи администраторов входит персонализация, резервное копирование и разблокировка электронных ключей. Для этих целей существует Мастер код. Все остальные действия, такие как занесение учетных записей в память электронного ключа, могут быть выполнены пользователем, владеющим ПИН кодом. Без правильного предъявления ПИН кода (если он поддерживается аппаратно) чтение секретной информации невозможно. После нескольких неправильных попыток предъявления ПИН блокируется (опять же, если реализовано

аппаратно). ПИН код может быть отключен. Мастер код так же может блокироваться, но в этом случае блокировка необратима. Мастер код открывает полный доступ ко всему электронному ключу или области памяти, выделенной для приложения ESMART® Access. Как правило, он одновременно является и транспортным кодом.

Вся информация в электронном ключе условно разбита на файлы, каждому из которых назначены атрибуты доступа. Электронный ключ хранит следующую информацию:

- Имя владельца (до 96 символов). Для изменения имени владельца требуется Мастер код. Чтение возможно всегда.
- Настройки пользователя (признак отключения ПИН кода, номер учетной записи для авто-входа и т.д.). Изменение возможно после проверки ПИН, чтение – всегда.
- Файл учетных записей пользователя для входа в систему. Содержит записи, состоящие из имени пользователя, домена и пароля. Чтение и запись возможны после предъявления ПИН. Файл может отсутствовать.
- Файл менеджера паролей. Содержит два рода парольных записей : парольные записи окон, включающие в себя имя пользователя, пароль и описание окна, позволяющее его распознать как объект для применения записи, и парольные записи WEB, содержащие описание WEB-формы для автоматического заполнения данными, хранимыми в памяти электронного ключа. Файл может отсутствовать.
- Файл электронного блокнота. Может содержать произвольный текст. Чтение и запись возможны после предъявления ПИН. Файл может отсутствовать.

Начальная инициализация структуры данных и файлов производится при выполнении операции разметки. Разметка требует предъявления Мастер кода. На стадии разметки задается начальный ПИН код, создаются и инициализируются обязательные файлы. Разметка полностью стирает текущую структуру данных в электронном ключе и воссоздает ее заново с потерей всей хранимой ранее информации.

Некоторые виды электронных ключей могут быть размечены для использования в других приложениях в дополнение к ESMART® Access. В этом случае доступно несколько шаблонов разметки.

Файлы данных пользователя так же создаются при разметке, но являются опциональными, то есть могут отсутствовать. Администратор может произвольно распределить память электронного ключа, выбирая размеры файлов данных или исключая их вовсе.

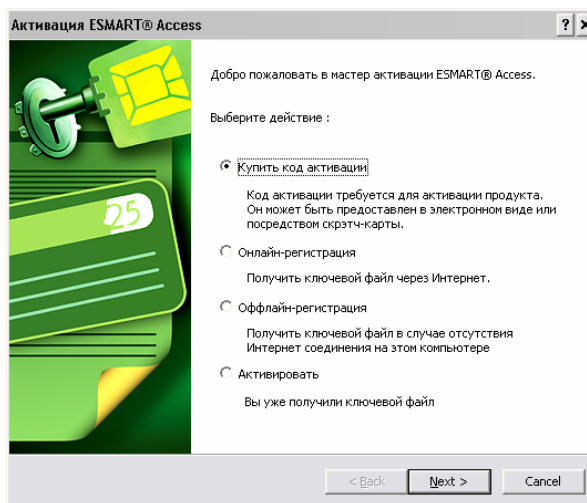
Раздел 3. Активация ESMART® Access

Для активации ESMART® Access необходимы файл и код подтверждения активации. Их Вы можете получить, выполнив процедуру регистрации через Интернет в online или offline режиме. Для успешного прохождения процедуры регистрации вам потребуется код активации вида *EAI-12345-1234567890*. Его Вы получаете тем или иным способом при покупке программного продукта, например посредством скрэтч-карты. Выполнив однажды процедуру активации и получив файл и код подтверждения активации, Вы можете сохранить их. Если потребуется активировать продукт еще раз, Вы сможете воспользоваться сохраненной копией.

Активация ESMART® Access может быть выполнена в программе ESMART® Access : Administrator. Чтобы начать выполнение любого действия, связанного с активацией продукта, выберите пункт меню “Справка->Активировать продукт”.

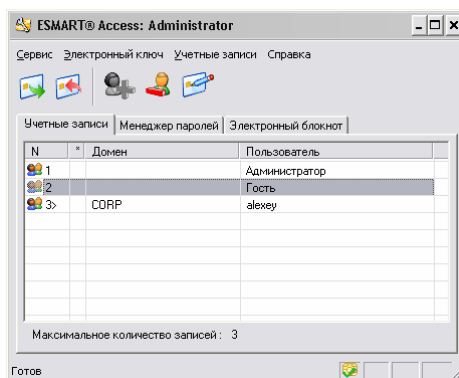
Мастер активации ESMART® Access позволит Вам быстро и комфортно активировать продукт. Активация состоит из трех шагов :

- 1) Приобрести код активации.
- 2) Выполнить регистрацию продукта через Интернет.
- 3) Активировать продукт.



Раздел 4. Работа с программой ESMART® Access : Administrator

Общие принципы работы с программой



Интерфейс программы ESMART® Access : Administrator включает в себя основное меню, панель инструментов и рабочую область. Основное меню позволяет задействовать все существующие функции. Для ускорения доступа к отдельным, наиболее часто используемым функциям, служит панель инструментов. Подводя курсор мыши к элементам панели инструментов, Вы можете получить по ним подсказку.

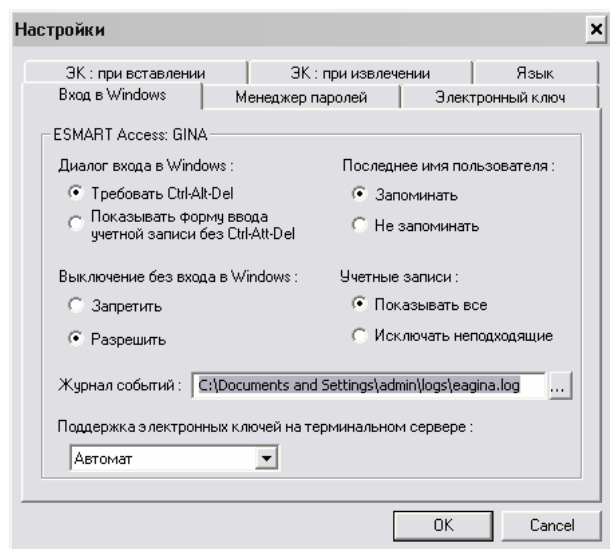
Рабочая область позволяет просматривать и редактировать пользовательскую информацию, хранимую в памяти электронного ключа, и состоит из закладок “Учетные записи”, “Менеджер паролей” и “Записная книжка”. Операции загрузки и сохранения данных, вызываемые из основного меню или из панели инструментов, работают с текущей закладкой.

Редактирование производится в режиме “offline”. После внесения изменений необходимо их сохранять.

Настройки

Диалог настроек можно вызвать из меню “Сервис->Настройки”. Настройки разделены по тематическим закладкам. Внутри закладки идет дальнейшее разделение по компонентам системы, к которым относятся настройки. Если вы не обладаете правами администратора на компьютере, то для редактирования будут доступны только настройки, индивидуальные для текущего пользователя операционной системы и относящиеся исключительно к программам ESMART® Access: Administrator и ESMART® Access: Tray.

Вход в Windows

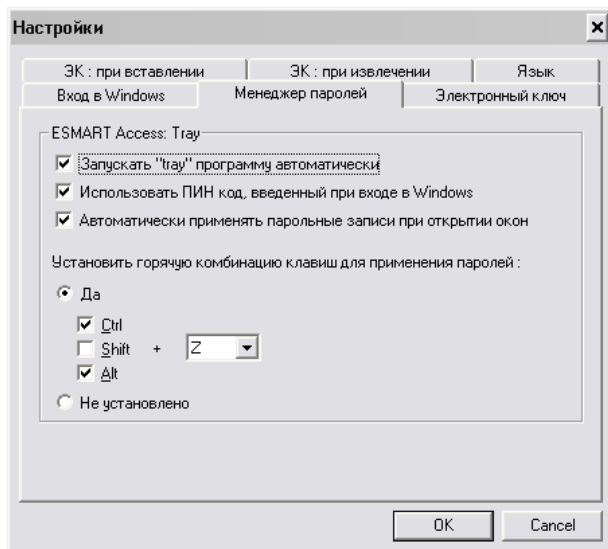


- **Требовать Ctrl-Alt-Del.** Если опция включена, то диалог ввода имени пользователя и пароля или ПИН кода появляется только после нажатия Ctrl-Alt-Del или вставки электронного ключа соответственно. Иначе заставка исключается, и Вы сразу видите приглашение ввести пароль или ПИН код. В Windows® 2000 Professional и Windows XP по умолчанию опция отключена.
- **Выключение без входа в windows.** Установка разрешает или запрещает выключение компьютера или перезагрузку без регистрации в системе. Как правило, выключение без регистрации разрешено на клиентских станциях и запрещено на серверах.
- **Запоминать последнее имя пользователя.** Если опция включена, то при входе по паролю система предлагает последнее имя пользователя и домен, которые были использованы для регистрации.
- **Исключать неподходящие учетные записи.** При входе в ОС или разблокировке компьютера исключить из списка рассматриваемых записей те записи, домен которых не является именем текущего компьютера, именем домена, членом которого является текущий компьютер, или именем одного из доменов, с которыми установлены доверительные отношения. Данная опция

позволяет хранить на электронном ключе учетные записи для входа в разные, не связанные в домен компьютеры и в то же время избежать диалога выбора учетной записи.

- **Лог-файл.** Указывается имя текстового файла, в который сохраняется журнал входа в систему, блокировки компьютера и всех остальных операций, выполняемых ESMART® Access : GINA.
- **Поддержка терминальной сессии.** Если поддержка терминальной сессии включена, то это может существенно увеличить время загрузки компьютера. Установка “Авто” включает поддержку терминальной сессии только в том случае, если терминальный сервер или удаленный рабочий стол действительно включены. Однако, если вы включите удаленный рабочий стол в процессе работы, модуль ESMART® Access : GINA не сможет адекватно отреагировать на это событие, и электронные ключи не будут поддерживаться в терминальной сессии до перезагрузки компьютера. Опция “включить только в ТС” – наилучший вариант для сервера, где используется только удаленный вход по электронным ключам.

Менеджер паролей

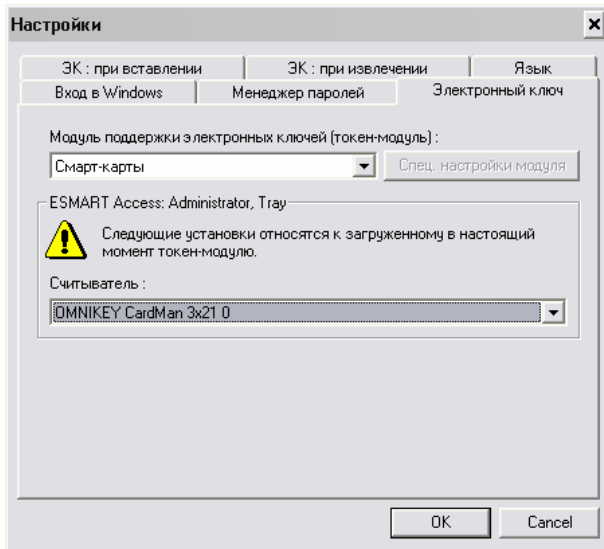


- **Запускать “tray” программу автоматически.** Если вы не пользуетесь функциями менеджера паролей, то в целях экономии ресурсов компьютера рекомендуется исключить “tray” программу из автозапуска.
- **Использовать ПИН код, введенный при входе в Windows.** Данная опция позволяет реализовать концепцию единого входа : вы авторизуетесь по электронному ключу только однажды – при входе в Windows. Дальнейшее применение паролей к прикладным программам и WEB-сайтам происходит прозрачно без дополнительного ввода ПИН кода. Однако, в случае использования этой возможности ПИН код может быть прочитан любой программой, выполняемой в контексте текущего пользователя, что может отрицательно сказаться на уровне безопасности.
- **Автоматически применять парольные записи при открытии окон.** Если включено автоматическое применение паролей, то ESMART® Access : Tray автоматически подгружает парольные записи при вставлении электронного ключа. При этом может появиться окно ввода

ПИН кода. В дальнейшем отслеживаются все открытия окон. Если какое-либо окно попадает под шаблон парольной записи, срабатывает процедура применения пароля.

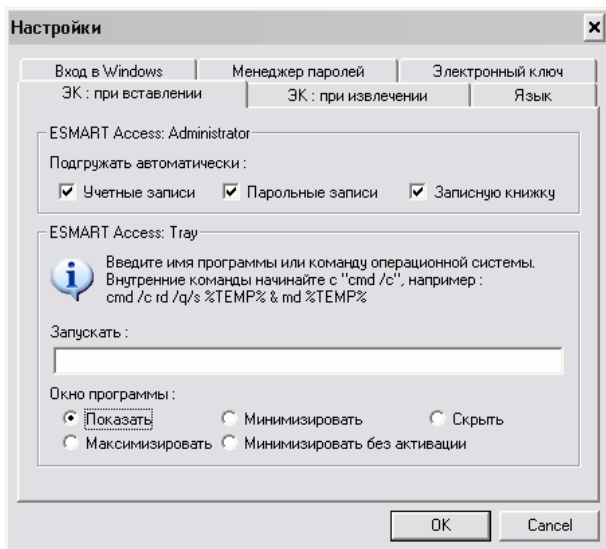
- **Горячая комбинация клавиш для применения паролей.** Позволяет быстро применить пароль в случае, если режим автоприменения отключен. Во избежание конфликтов с другими программами, а так же для удобства пользователя, комбинация может переназначаться. По умолчанию устанавливается Ctrl+Alt+Z.

Электронный ключ

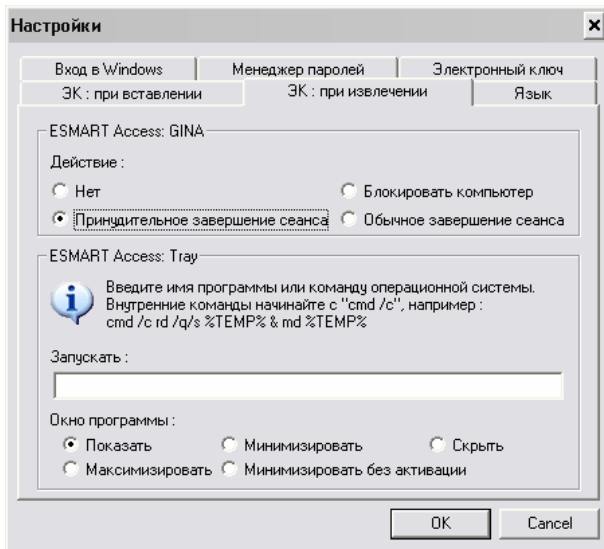


- **Модуль поддержки электронных ключей.** Выберите из списка используемый Вами тип устройств. В списке доступны только те устройства, модули поддержки которых установлены в настоящий момент и лицензированы для использования.
- **Специальные настройки токена-модуля.** Специальные настройки, относящиеся только к загруженному в настоящий момент токен-модулю. Подробнее о настройках отдельных модулей читайте в разделе описания модулей. Специальные настройки доступны не для всех модулей.
- **Считыватель.** Программы ESMART® Access: Administrator и ESMART® Access: Tray могут работать только с одним считывателем одновременно. Если у Вас установлено несколько считывателей (в т.ч. виртуальных, создаваемых драйверами USB токенов), выберите нужный.

ЭК: при вставлении

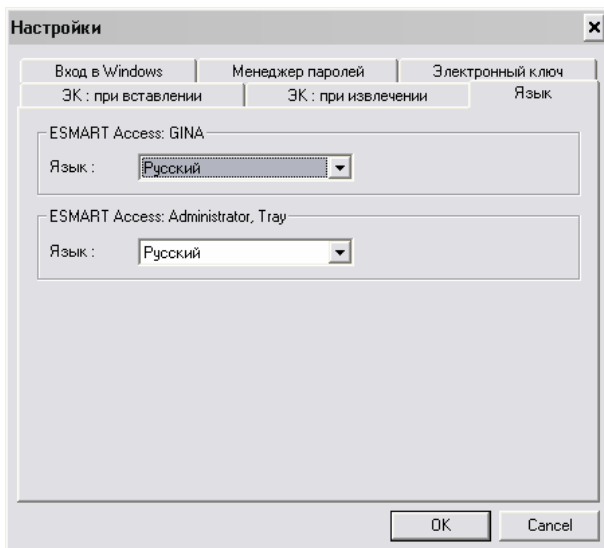


ЭК: при извлечении



- **Действие.** Если вход в систему осуществлен посредством электронного ключа, то Вы можете определить реакцию системы при его извлечении. Используйте опцию “обычное завершение сеанса” только в случае особой необходимости : в этом случае нет гарантии, что сеанс будет действительно завершен.

Язык



- **Язык.** Возможно разделить настроить язык интерфейса входа в операционную систему и язык программ Administrator и Tray.

Разметка электронных ключей

Перед использованием электронный ключ должен быть размечен. Для начала разметки вставьте его в считыватель. Если электронный ключ ранее не размечался, то программа автоматически предложит его разметить. Если этого не произошло, то выберите пункт меню “Электронный ключ -> Разметить”.

Разметка электронного ключа

Разметка
 Изменение кода
 Учетные записи
 Менеджер паролей
 Электронный блокнот

Перед использованием электронный ключ должен быть размечен.

[Введите Мастер код](#) : [masked] HEX формат

Выберите шаблон разметки :
ESMART Access Net

[Введите начальный ПИН](#) : [masked] ПИН отключен

Подтверждение ПИН : [masked]

Введите имя владельца электронного ключа (до 36 символов):
Радюков Иван Андреевич

ВНИМАНИЕ! Нажатие "Далее" сотрет все имеющиеся записи в электронном ключе

< Назад **Далее** > Отмена

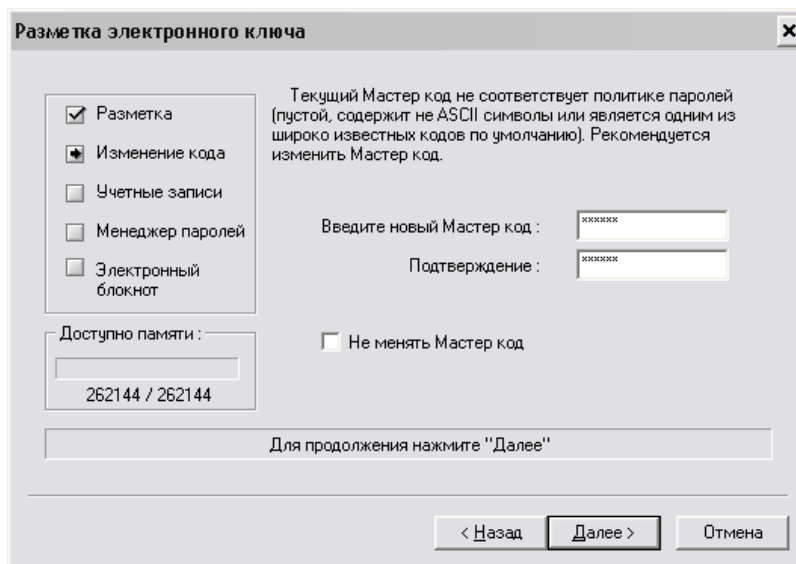
Для разметки необходимо знать текущий Мастер код. Если электронный ключ ранее не размечался, то Мастер код соответствует транспортному коду электронного ключа. Список транспортных кодов по умолчанию и другую справочную информацию можно получить, кликнув ссылку, помеченную синим цветом. Для некоторых электронных ключей транспортный код по умолчанию не может быть введен с клавиатуры в символьном виде. В этом случае необходимо ввести код в шестнадцатеричном (HEX) формате. Длина кода всегда 8 байт или 16 шестнадцатеричных цифр.

Шаблон разметки позволяет выбрать дополнительные опции, позволяющие использовать электронный ключ в других приложениях совместно с ESMART® Access.

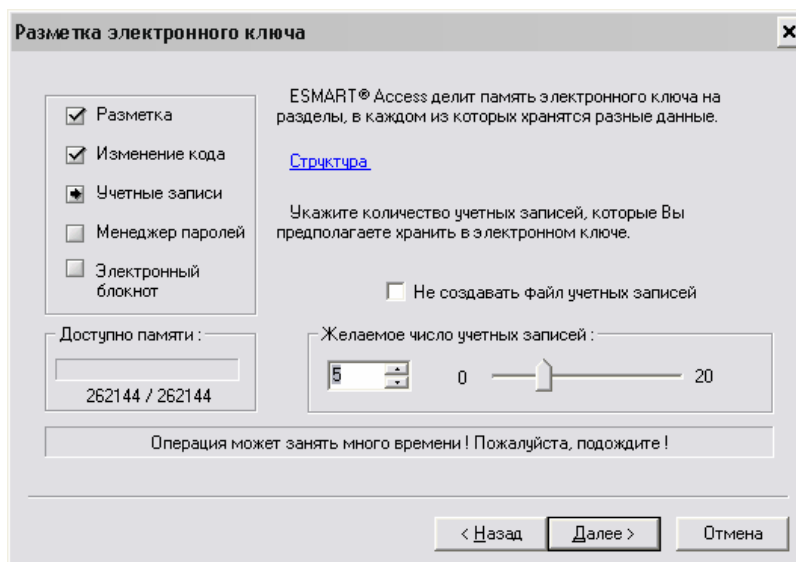
При разметке всегда происходит сброс ПИН кода на некоторое начальное значение, задаваемое администратором. При желании можно отключить ПИН код.

Имя владельца электронного ключа задается администратором и не может быть изменено пользователем, но всегда может быть прочитано. Следовательно, независимо от действий пользователя, электронный ключ всегда может быть идентифицирован.

После нажатие кнопки “Далее” происходит уничтожение текущей информационной структуры, хранимой в памяти электронного ключа. Все данные теряются!

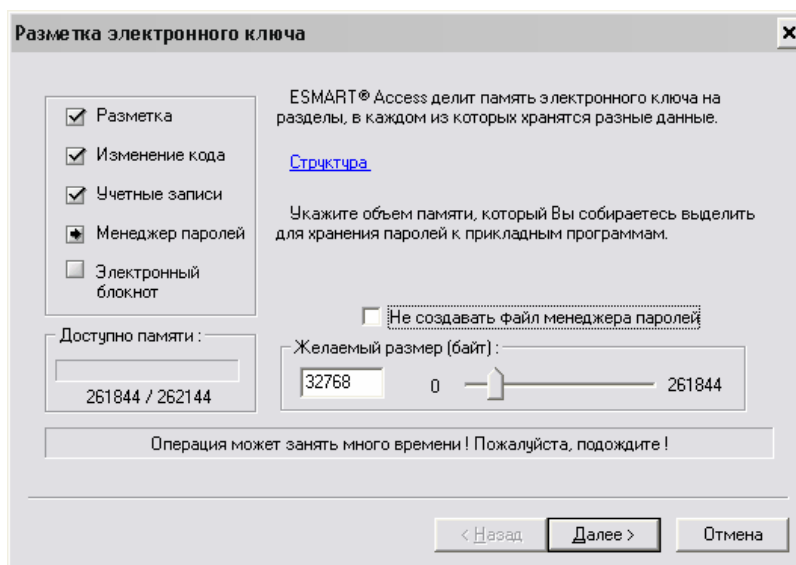


Если текущий Мастер код не может быть введен с клавиатуры или является широко известным ключом, то мастер попросит Вас поменять Мастер код. Вы можете оставить его без изменений, **но тем самым Вы подвергаете информационную безопасность серьезному риску!** Если Вы оставите не ASCII ключ, то из программ ESMART® Access Вам будут недоступны все функции, требующие предъявления Мастер кода.

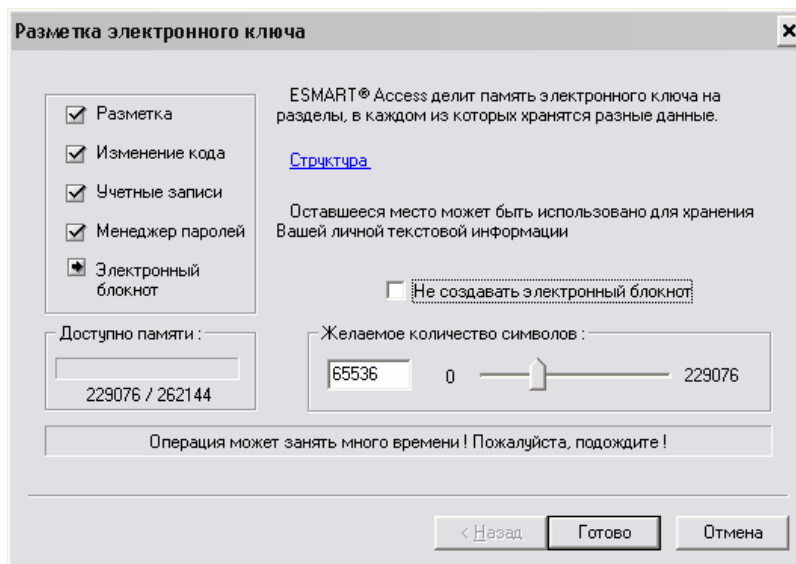


Все дальнейшие операции являются необязательными. Однако, если Вы не создадите никаких пользовательских файлов, электронный ключ будет бесполезен. При создании файлов

продумайте как он будет использоваться. Если электронный ключ предназначен для обычного пользователя, которому предоставлена одна учетная запись в системе, но ему необходимо хранить много паролей к различным программам или нужна большая записная книжка, то имеет смысл сделать файл учетных записей размером в одну запись, а все остальное место оставить под другие файлы. По умолчанию размер – 5 записей, если только для них достаточно памяти, иначе - максимально доступное количество. После создания файла его размер не может быть изменен без переформатирования.



По умолчанию половина оставшейся памяти выделяется под менеджер паролей, но не более 32Кб. Если Вам не нужна записная книжка, то рекомендуем увеличить размер файла менеджера паролей до максимума.



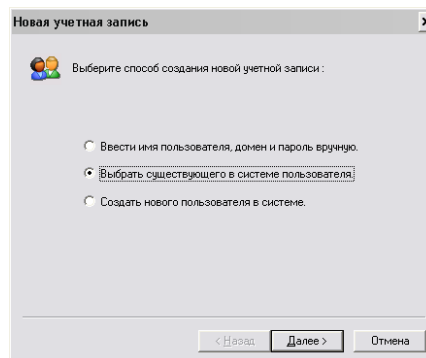
Записная книжка позволяет хранить произвольный текст в памяти электронного ключа. Заметки, номера телефонов, адреса, пароли и многое другое. Если Вам не нужна записная книжка, Вы можете отказаться от ее создания, тем самым, освобождая дополнительную память для других целей.

Создание учетных записей

После разметки электронный ключ не содержит учетных записей и не может быть использован для регистрации в операционной системе. Для этого нужно сначала создать одну или несколько учетных записей, включающих в себя имя пользователя, имя домена и пароль. Чтобы создать учетную запись, выберите пункт меню “Учетные записи -> Новая учетная запись” или нажмите соответствующую кнопку в панели инструментов.

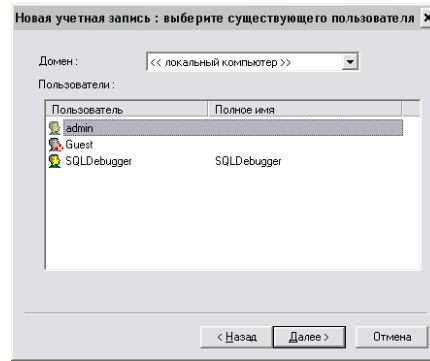
У вас есть 3 варианта:

- Ввести имя пользователя, имя домена и пароль вручную. При этом не контролируется правильность вводимой информации;
- Выбрать существующего в системе пользователя и ввести его пароль;
- Создать нового пользователя в системе и прописать его в электронный ключ;

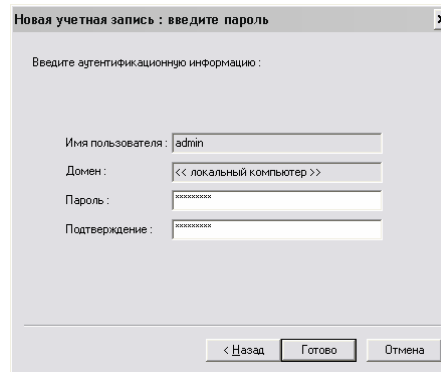


Остановимся подробнее на двух последних вариантах.

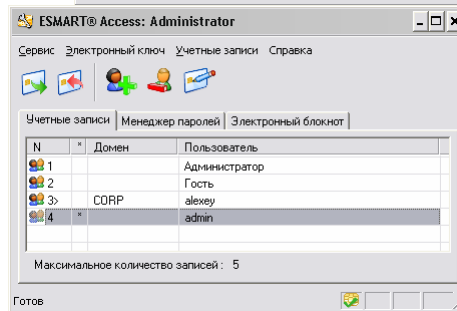
Чтобы прописать в электронный ключ существующего пользователя, надо выбрать из списка домен, в котором находится пользователь. При этом будет показан список пользователей выбранного домена. Отметьте нужного пользователя и нажмите “Далее”.



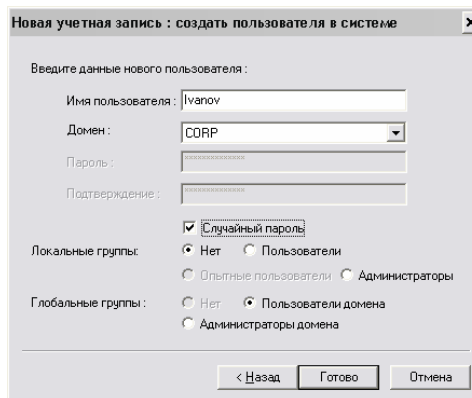
Введите дважды пароль пользователя и нажмите “Готово”. Запись будет помещена в редактор учетных записей.



Звездочка в графе “*” означает, что запись или порядковое положение записи были изменены и требуется сохранение записей в электронный ключ. Для сохранения нужно выбрать пункт меню “Сервис->Сохранить информацию в электронный ключ”. Для удобства воспользуйтесь панелью инструментов или просто нажмите Ctrl+S.



При создании нового пользователя нужно выбрать для него имя длиной до 20 символов, домен, в котором будет создан пользователь, назначить пароль и права доступа. Пароль рекомендуется делать случайным. В этом случае он будет состоять из беспорядочного длинного набора символов, что практически исключит возможность перебора.



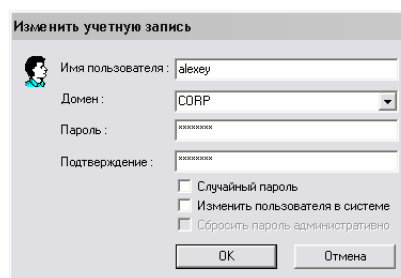
Из программы можно назначить только базовые права доступа, а именно членство во встроенных в систему локальных и глобальных группах: Users, Power Users, Administrators, Domain Users, Domain Admins. Если требуется более тонкая настройка прав, то вы всегда можете это сделать средствами операционной системы. Глобальные группы доступны только в том случае, если создается доменный пользователь.

Создание и модификация пользователей в операционной системе текущего компьютера, возможна только пользователями, обладающими правами локального администратора. Создание и модификация пользователей в домене возможна только с компьютеров-членов домена или trusted домена, обладающими правами локального администратора на домен-контроллере того домена, к которому принадлежит учетная запись. Как правило это пользователи, принадлежащие группе “Domain admins” или “Enterprise admins”.

Обратите внимание : ESMART® Access не работает с DNS именами доменов (например, office12.spb.corp.ru). Используйте имена доменов в стиле NETBIOS.

Редактирование учетных записей

Самый простой способ вызова записи на редактирование – двойной клик на записи в списке.



Если Вы хотите изменить пароль пользователя в операционной системе, пометьте флажок “изменить пользователя в системе”. Изменение возможно двумя способами: обычная смена пароля (не требует привилегий администратора, но требует соответствия текущего пароля в электронном ключе и в системе) и административная (требуются права администратора, но правильность текущего пароля не имеет значения).

Внимание! Если Вы изменили учетную запись в системе, то обязательно нужно сохранить файл учетных записей в электронном ключе! Иначе нарушится соответствие пароля в токене и в системе, и вход станет невозможным! Если все же это произошло, то воспользуйтесь административным сбросом пароля.

Внимание! Административная смена пароля может лишить пользователя доступа к защищенным данным, хранящимся в его профиле. В том числе, пользователь потеряет доступ к зашифрованным средствами NTFS файлам !

Удаление учетных записей

Чтобы удалить одну или несколько учетных записей, отметьте их в списке и выполните одно из следующих действий:

- Нажмите клавишу “Del”;
- В контекстном меню выберите пункт “Удалить”;
- В основном меню выберите пункт “Учетные записи->Удалить”;
- Нажмите кнопку на панели инструментов со знаком “-“.

Учетные записи не удаляются из операционной системы! Для этого воспользуйтесь средствами ОС.

Автоматический выбор учетной записи

Если в электронном ключе прописано несколько учетных записей, то при входе в систему Вам будет предложен список доступных записей. Если Вы не хотите удалять другие записи, но хотите, чтобы вход в систему происходил только по одной из них, Вы должны пометить запись для авто-входа. Для этого нужно выбрать пункт контекстного меню “пометить для авто-входа” или пункт основного меню “Учетные записи -> пометить для авто-входа”. Отмеченная запись помечается знаком “>” в колонке номера записи (например, “2>”). Чтобы отменить авто-вход, выберите пункт меню “Отменить авто-вход”.

Менеджер паролей

Существует огромное множество программ, использующих пароли как средство авторизации доступа. Пароли могут применяться для доступа в Интернет через модем, к различным сайтам, документам, файлам и базам данных. Сколько программ, столько и разных форматов хранения данных, программных интерфейсов, несовместимых между собой.

То единственное общее, что позволяет автоматизировать процесс ввода паролей для разных программ,- это окна графического интерфейса пользователя. Как правило, ввод паролей осуществляется в специальных окнах – диалогах в поля ввода текста. Практически для каждого окна можно найти уникальный набор критериев, позволяющих уверенно опознать это окно как объект ввода определенного набора данных. ESMART® Access позволяет привязаться к следующим элементам окна:

- текст заголовка окна;
- текст и расположение произвольной статической надписи;
- текст и расположение кнопки подтверждения ввода;
- расположение поля ввода имени пользователя;
- расположение поля ввода пароля.

Под “расположением” понимается внутренний набор данных, позволяющий найти элемент управления в диалоговом окне. Расположение не может быть введено или изменено пользователем с клавиатуры, но может быть получено в процессе выбора окна курсором мыши.

Критерии привязки могут произвольно сочетаться, некоторые из них могут отсутствовать, однако привязка к полю ввода имени пользователя или пароля должна присутствовать. Совокупность критериев привязки называется шаблоном привязки к окну. Окно соответствует шаблону, если выполняются все критерии привязки. Шаблон обязательно содержит привязку к окну, но может не содержать фактических имени пользователя и пароля. Запись, содержащая фактические данные называется парольной записью. Парольные записи непосредственно сохраняются в электронный ключ и используются для применения паролей к окнам. Для сокращения объема памяти из парольных записей исключается полный текст элементов управления – сохраняются лишь несколько байт, позволяющих сравнить реальный текст с эталоном. Шаблоны дают возможность ускорить процесс создания парольных записей – достаточно лишь выбрать шаблон и указать фактические данные для ввода в форму. Шаблоны хранятся в персональной ветке реестра текущего пользователя операционной системы и не записываются в электронный ключ. Чтобы скопировать шаблоны для другого пользователя ОС или на другой компьютер, необходимо выполнить экспорт и импорт шаблонов.

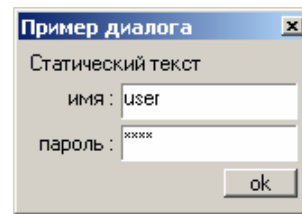
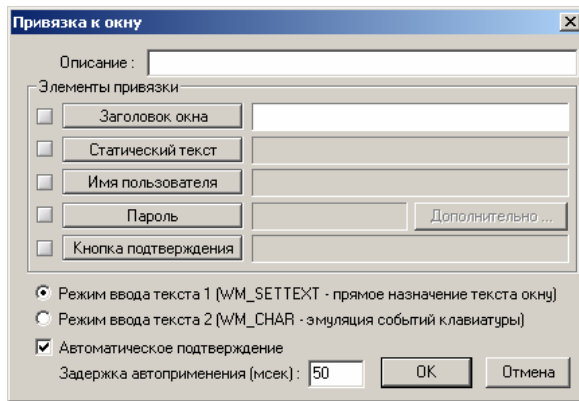
В дополнение к парольным записям для окон, с версии 1.411 поддерживается другой тип парольных записей – парольные записи WEB. Они предназначены для автоматизации заполнения форм на WEB-сайтах в браузерах Internet Explorer 5.0 и 6.0.

Парольные записи WEB выделены в отдельный класс парольных записей не случайно. Во-первых, элементы управления WEB сайтов не являются классическими окнами Windows®. Поэтому менеджер оконных парольных записей просто не замечает поля WEB форм. Во-вторых, кроме имени пользователя и пароля, довольно часто требуется указание дополнительных параметров в WEB форме. Например, на сайте <http://www.mail.ru> от Вас потребуют ввести доменное имя вашего email. ESMART® Access позволяет работать с формами любого размера, содержащими любые элементы, предусмотренные в стандарте HTML. Поэтому Вы можете автоматизировать не только парольный вход на сайт, но и вообще автоматизировать заполнение любых форм.

Редактирование парольных записей

Операции редактирования парольных записей и шаблонов выполняются в программе ESMART® Access : Administrator. Новая парольная запись может быть создана из меню “Парольные записи” или посредством панели инструментов. Рассмотрим процесс создания парольной записи на примере. Предположим, требуется сохранить пароль для доступа к Интернет сайту <http://www.windowsmedia.com>. Последовательность действий может быть следующей:

1. Вызовите диалог создания новой парольной записи;



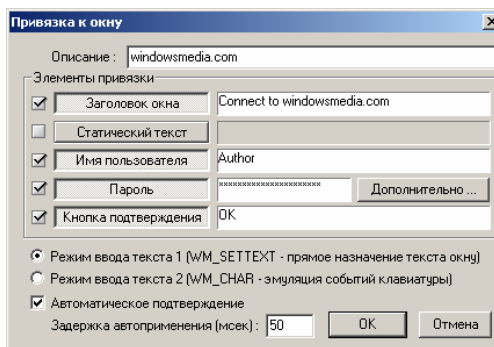
- Откройте браузер, зайдите на нужный сайт, чтобы появилось окно, куда Вы должны вводить имя пользователя и пароль;



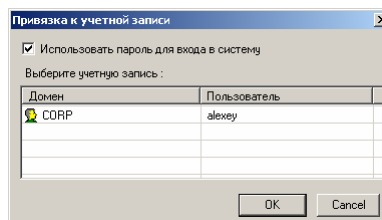
- Определите необходимый набор критериев привязки к окну. Чем больше критериев привязки, тем меньше возможностей для ложного срабатывания. Однако, тем и больше объем памяти, требуемый для хранения парольной записи. В данном случае достаточно привязаться к заголовку окна, так как другое окно с таким заголовком вряд ли может иметь место. Опишем процесс привязки к элементу управления на примере заголовка окна (точно так же выполняется привязка к статической надписи и всем остальным элементам).

 - Нажимаем кнопку "Заголовок окна". Окна ESMART® Access пропадают, а курсор меняет свой вид на прицел.
 - Удерживая левую кнопку мыши, подводим прицел к интересующему нас элементу. Выбранный элемент подсветится темной рамкой. Если этого не произошло, значит выбранный элемент не соответствует нужному типу. В правом нижнем углу экрана показывается пример диалога, где нужный элемент мигает, тем самым подсказывая куда нужно вести курсор.
 - Отпускаем кнопку мыши. Появляются окна ESMART® Access вместе с диалогом привязки к окну. Информация об элементе автоматически копируется в окно привязки.

Аналогичным способом привяжитесь к полям ввода имени пользователя и пароля.



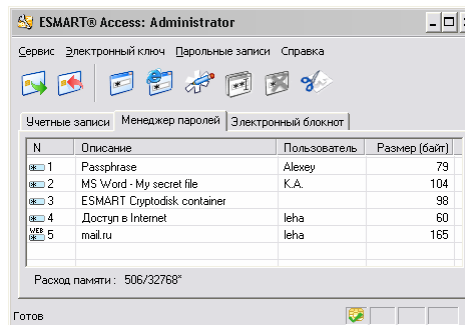
4. Задайте фактические имя пользователя и пароль. Их нужно ввести в поля ввода формы привязки к окну. Также, если пароль к данной программе совпадает с паролем пользователя к учетной записи – можно выбрать кнопку «Дополнительно...» и отметить пункт «Использовать пароль для входа в систему», также отметив пользователя, пароль которого необходимо вводить в окно.
5. Если Вы желаете, чтобы ввод пароля автоматически подтверждался, пометьте соответствующий флажок. Автоматическое подтверждение без привязки к кнопке ввода не всегда возможно. Если Вы увидите, что авто-подтверждение не срабатывает, то привяжитесь к кнопке ввода. Это должно решить проблему.
6. Случается так, что сразу после открытия окно еще не готово принимать вводимую информацию. Если ввод не срабатывает или срабатывает неустойчиво, попробуйте установить задержку 50-100 мс.
7. Некоторые программы используют нестандартные окна ввода текста, из-за чего менеджеру паролей не удастся правильно вставить текст в окно. В ряде случаев проблема решается за счет максимального подражания человеку – эмуляции нажатий на клавиши. Если режим ввода текста 1 не работает или работает неправильно, попробуйте установить режим 2.
8. (Опционально) Опишите как-нибудь запись, чтобы потом можно было понять для чего она нужна. Этого можно и не делать - тем самым экономится память.



После создания записи она помещается в список.

Комментарий к примеру: следует различать ввод пароля на сайт в окно web документа (форму) и отдельный диалог авторизации пользователя. Привязка к элементам web документа невозможна в рамках оконных парольных записей, т.к. они не являются стандартными окнами Windows®.

Парольные записи имеют переменный формат и могут занимать разный объем памяти. Размер каждой записи можно увидеть в правой колонке. Внизу показывается общий расход памяти в виде <занято>/<всего>. Символ “*” означает то, что список был модифицирован и требуется сохранение. Пока список не будет сохранен, программа ESMART® Access : Tray не увидит изменений.

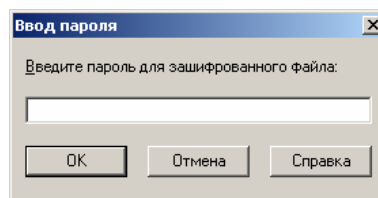


Чтобы отредактировать запись, дважды щелкните по ней мышью или воспользуйтесь меню или панелью инструментов. Текст элементов привязки “заголовок”, “статическая надпись”, “кнопка ввода” не будет отображен. Это происходит потому, что в парольной записи в целях экономии памяти не сохраняется полный текст. Вы можете вписать другой текст или заново привязаться к элементу. Любая модификация строчки “<...текст элемента управления определен...>” впишет новый текст в таком виде, который отображен в строке.

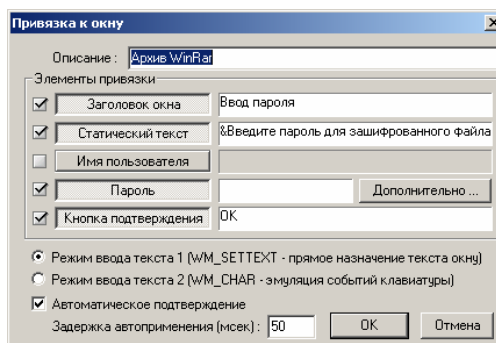
Создание и редактирование шаблонов

Шаблоны позволяют существенно упростить и ускорить процесс создания парольных записей. В самом деле, любая парольная запись состоит из двух частей – привязки к окну и фактических данных об имени пользователя и пароле. Привязка не меняется для одной и той же программы и при использовании одного и того же ресурса. Если Вы планируете сохранять разные пароли к одной и той же программе или к одному и тому же ресурсу, то имеет смысл создать шаблон. Шаблон создается в редакторе шаблонов, который вызывается из основного меню или панели инструментов.

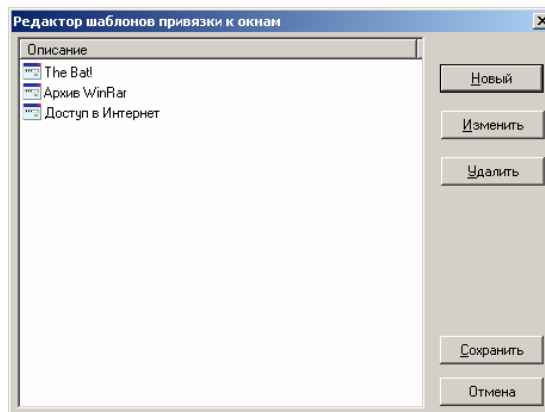
Предположим, что нужно сохранять пароли для RAR архивов. Вызовите окно ввода пароля WinRar.



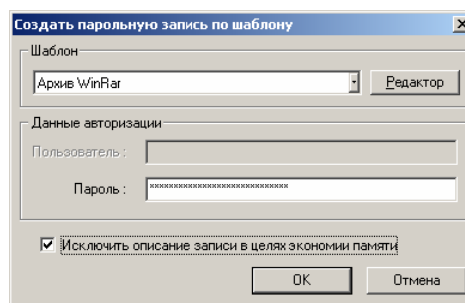
Для создания шаблона в редакторе шаблонов нажмите кнопку “Новый”.



Определите критерии привязки к окну описанным ранее способом, но **не вписывайте фактический пароль**. Нажмите “ОК”. Шаблон появится в списке.



Сохраните шаблоны. Теперь чтобы создать парольную запись для WinRar выберите пункт меню “Новая запись по шаблону”.



Выберите шаблон из списка, введите пароль и парольная запись готова! Не надо опять открывать окно ввода пароля, не надо привязывать элементы управления и придумывать набор критериев. Нужно только ввести еще один пароль.

Парольные записи, созданные по шаблону, далее никак от него не зависят. Например, администратор может создать для пользователя парольную запись для доступа к электронной почте на своем компьютере. Пользователь сможет применить запись на любом другом компьютере, даже если там нет никаких шаблонов или программа администратора не установлена вовсе.

Экспорт и импорт шаблонов

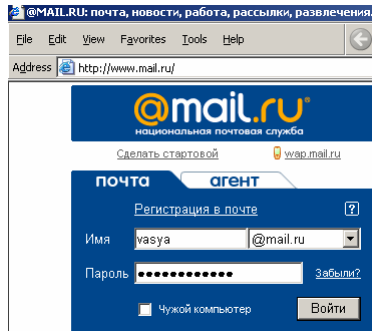
Шаблоны хранятся на текущем компьютере в области реестра текущего пользователя ОС. Если необходимо перенести шаблоны на другой компьютер, сделать их доступными другому пользователю или создать резервную копию, нужно экспортировать шаблоны в файл. Это делается из меню “Парольные записи->Экспортировать шаблоны”.

При импорте шаблонов Вам будет предложено 2 опции: добавить шаблоны к текущим или заместить их. В последнем случае текущие шаблоны будут удалены. Если нужно добавить только часть шаблонов, то выберите опцию “Добавить”, а после импорта вручную удалите ненужные шаблоны.

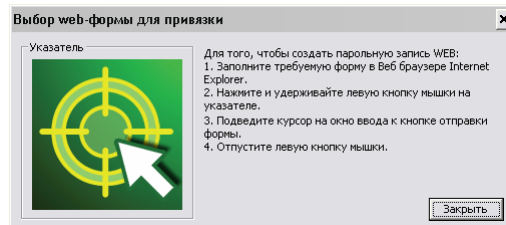
Редактирование парольных записей WEB

Операции редактирования парольных записей WEB выполняются в программе ESMART® Access : Administrator. Новая парольная запись может быть создана из меню “Парольные записи” или посредством панели инструментов. Рассмотрим процесс создания парольной записи на примере. Предположим, требуется сохранить пароль для доступа к почтовый ящик vasya@mail.ru. Последовательность действий может быть следующей:

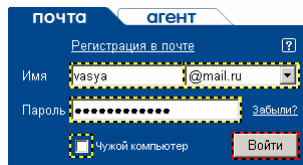
1. Откройте браузер, зайдите на нужный сайт, чтобы появилась страница, куда Вы должны вводить Ваши данные. В нашем примере – это <http://www.mail.ru>.
2. Заполните WEB форму. Форма должна быть уже заполнена перед привязкой к парольной записи.



3. Вызовите диалог создания новой парольной записи WEB в менеджере паролей.



4. Подведите курсор мыши к указателю в форме прицела и нажмите левую кнопку мыши. Окна ESMART® Access пропадут, а курсор поменяет свой вид.
5. Удерживая левую кнопку мыши, наведите курсор на любой элемент управления необходимой WEB-формы. При этом подсветятся все элементы выбранной формы.



- Отпустите кнопку мыши. Появятся окна ESMART® Access вместе с диалогом привязки к WEB форме.

Имя	Тип	Значение
<input checked="" type="checkbox"/> Login	input:text	vasya
<input checked="" type="checkbox"/> Domain	select	mail.ru
<input checked="" type="checkbox"/> Password	input:password	*****
<input checked="" type="checkbox"/> level	input:checkbox	1

Имя	Тип	Надпись
<input checked="" type="checkbox"/>	input:submit	Войти

Автоматическая отправка формы
 Отправлять форму автоматически
Кнопка подтверждения: ;input:submit (Войти)

- По умолчанию парольная запись не настраивается на автоматическую отправку формы. Это сделано, чтобы в случае ошибки предотвратить бесконечную отправку одной и той же информации в Интернет. Если Вы хотите отправлять форму автоматически после ее заполнения, пометьте флажок “отправлять форму автоматически”.
- Обратите внимание, что по умолчанию устанавливается критерий распознавания WEB формы – URL документа. Если Вы привязали парольную запись, зайдя на сайт <http://www.mail.ru>, то она не будет применяться на сайте <http://mail.ru>, хотя по смыслу это один и тот же сайт. Если необходимо, чтобы распознавание формы происходило независимо от Интернет-адреса, снимите пометку флажка “URL документа”.
- (Опционально) Опишите как-нибудь запись, чтобы потом можно было понять для чего она нужна. Этого можно и не делать - тем самым экономится память.
- Впоследствии, если Вам нужно изменить пароль, не обязательно выполнять привязку к форме заново. Редактор парольных записей WEB позволяет изменять данные, вводимые в текстовые поля. Редактирование остальных полей не предусмотрено.

Программа ESMART® Access: Tray. Применение парольных записей

Применение в данном контексте означает анализ имеющихся парольных записей, поиск подходящего окна и вставку данных в окно. Применение записей реализуется отдельной программой, называемой ESMART® Access : Tray. Tray – это область рабочего стола в правом нижнем углу, куда часто помещаются иконки для быстрого доступа к резидентным программам. ESMART® Access : Tray так же создает иконку. Внешний вид иконки говорит о текущем состоянии электронного ключа.



- электронный ключ вставлен и парольные записи загружены;



- электронный ключ вставлен и парольные записи не загружены;



- электронный ключ вытасцен;



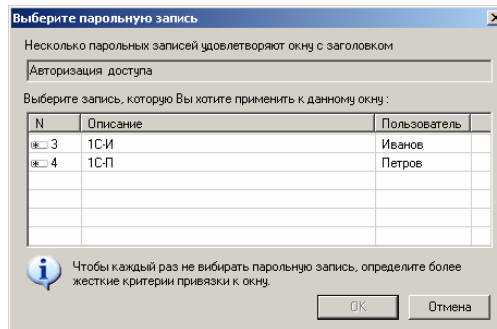
- токен-модуль недоступен или не работает.

Настройки системы управления электронными ключами являются общими для всех компонентов ESMART® Access, поэтому если возникают какие-то неполадки, лучше их диагностировать в программе ESMART® Access : Administrator.

Чтобы применить парольные записи нужно:

- Вставить электронный ключ. Иконка должна поменяться.
- При необходимости ввести ПИН код.
- Вызвать окно ввода пароля программы.
- Выполнить одно из действий: дважды кликнуть по иконке в tray, нажать горячую комбинацию клавиш (по умолчанию Ctrl+Shift+Z) или в tray-меню, вызываемом нажатием правой кнопки на иконке, выбрать “Применить пароли”.
- Ввести ПИН код (если он включен и не вводился ранее в ESMART® Access : Tray).

Если найдено окно, к которому подошла одна запись, то она будет применена сразу же. Если подошло несколько записей, то будет предложено выбрать из списка нужную запись. В графе номера отображается номер записи из полного списка, хранимого в электронном ключе.



Если найдено несколько окон, к которым подходят парольные записи, то работа осуществляется только с первым найденным окном. Если же не найдено ни одного совпадения, то просто ничего не произойдет.

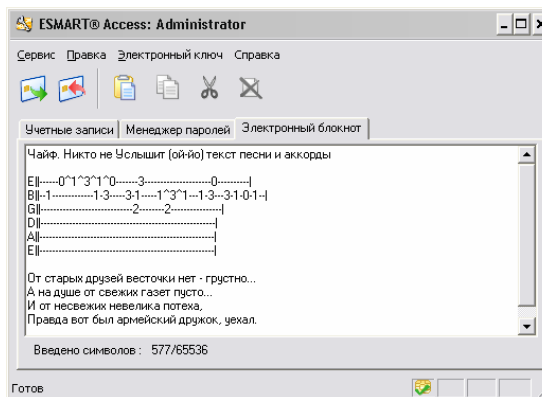
Настройка опций программы ESMART® Access: Tray и редактирование парольных записей осуществляется из программы ESMART® Access: Administrator. Хотя они и являются разными программами, они могут синхронизировать свою работу. Если Вы отредактировали и записали парольные записи, то не нужно перезапускать tray – администратор оповестит tray об изменении, и при следующем применении список будет загружен заново. То же касается и изменения ПИН-кода. Модуль входа в систему ESMART® Access : GINA не всегда может синхронизировать работу с программами, исполняемыми в контексте текущего пользователя. Если Вы меняете ПИН посредством ESMART® Access : GINA, а потом повторно обращаетесь к электронному ключу из ESMART® Access : Administrator или ESMART® Access : Tray, то код будет предъявлен один раз неправильно, что уменьшит счетчик оставшихся попыток ввода и вызовет окно запроса ПИН.

Горячая комбинация клавиш позволяет быстро применить пароль в случае, если режим автоприменения отключен. Во избежание конфликтов с другими программами, а так же для

удобства пользователя, комбинация может переназначаться. По умолчанию устанавливается Ctrl+Alt+Z.

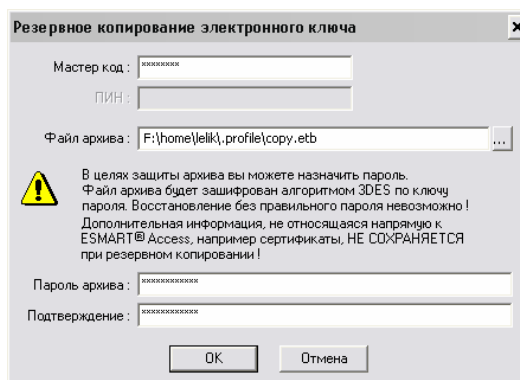
Редактирование записной книжки

Перейдите в закладку “Записная книжка”. Пользовательский интерфейс редактора практически полностью соответствует программе “Блокнот” (“Notepad”). Внизу выводится подсказка о размере записной книжки и количестве введенных символов. Для записи текста нажмите Ctrl+S, для загрузки – Ctrl+L.



Резервное копирование

Резервное копирование позволяет создавать копии электронных ключей пользователей с возможностью их последующего восстановления. В копию включается вся информация, относящаяся к приложению ESMART@ Access. Резервная копия может быть восстановлена и на другой электронный ключ, в т.ч. другого типа, при условии достаточности памяти для размещения всех файлов.



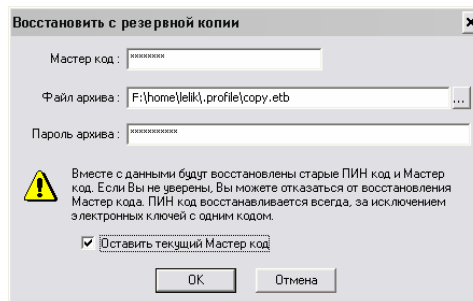
Чтобы начать резервное копирование выберите пункт основного меню “Сервис->Создать резервную копию электронного ключа”.

Для копирования электронного ключа необходимо знать Мастер код, а для некоторых типов ключей и ПИН код. Укажите имя файла архива. Желательно назначить пароль на архив, иначе любой, кто имеет доступ к файлу, сможет им воспользоваться.

Обратите внимание, что в копии сохраняются значения ПИН кода и Мастер кода. При последующем восстановлении коды будут изменены на те, что содержатся в копии. Если Вы восстановите копию, для которой забыли Мастер код, то электронный ключ будет заблокирован без возможности восстановления. Если вы не помните Мастер код для копии, то можно отказаться от смены Мастер кода.

Чтобы восстановить электронный ключ с резервной копии выберите пункт основного меню “Сервис->Создать резервную копию электронного ключа”.

В процессе восстановления производится форматирование. Текущая информация, содержащаяся в памяти ключа, теряется.

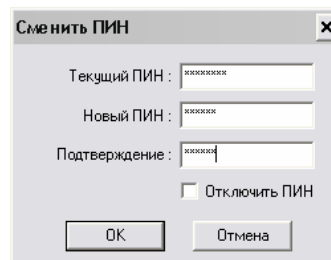


Операции с ключами доступа

Из программы ESMART® Access : Administrator можно:

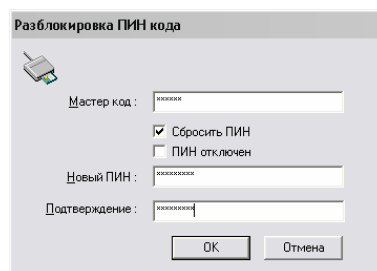
- Изменить ПИН код;
- Разблокировать или сбросить ПИН;
- Изменить Мастер код.

Все эти функции доступны из меню “электронный ключ”.



Чтобы сменить ПИН или Мастер код, необходимо предъявить их старые значения и дважды ввести новое значение, после чего нажать кнопку ОК. Отключение ПИН – понятие внутреннее для ESMART® Access. Как правило, отключенные и пустые ПИН коды несовместимы с другими приложениями.

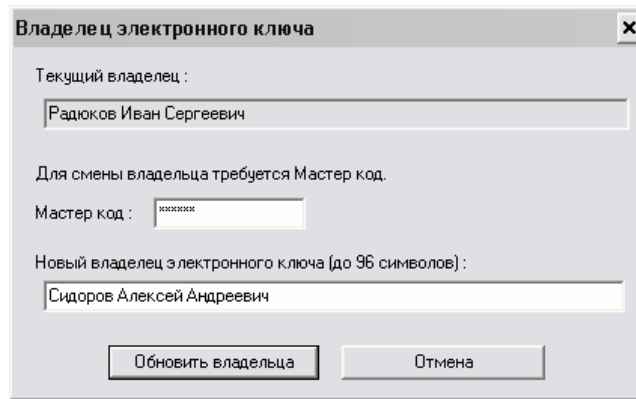
Если ПИН код заблокирован после нескольких неправильных попыток ввода, он может быть разблокирован по предъявлению Мастер кода. Если ПИН код утерян, то он может быть сброшен на произвольное значение или отключен.



Смена владельца электронного ключа

Выберите пункт меню “Электронный ключ - >Владелец”.

Просмотр текущего владельца не требует каких-либо привилегий. Для изменения владельца требуется предъявление Мастер кода.



Владелец электронного ключа

Текущий владелец :
Радоков Иван Сергеевич

Для смены владельца требуется Мастер код.

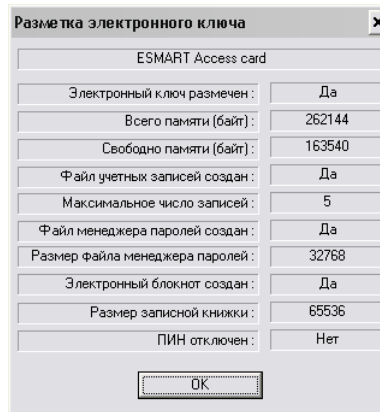
Мастер код : [xxxxxxx]

Новый владелец электронного ключа (до 96 символов) :
Сидоров Алексей Андреевич

Обновить владельца Отмена

Просмотр текущей разметки ключа

Чтобы получить информацию о текущей разметке электронного ключа выберите пункт основного меню “Электронный ключ->Показать разметку”.



Разметка электронного ключа

ESMART Access card

Электронный ключ размечен :	Да
Всего памяти (байт) :	262144
Свободно памяти (байт) :	163540
Файл учетных записей создан :	Да
Максимальное число записей :	5
Файл менеджера паролей создан :	Да
Размер файла менеджера паролей :	32768
Электронный блокнот создан :	Да
Размер записной книжки :	65536
ПИН отключен :	Нет

OK

Работа с модулем входа в систему ESMART® Access : GINA

Модуль ESMART® Access : GINA полностью заменяет стандартный Microsoft GINA (msgina.dll). Функционально пользовательский интерфейс почти полностью соответствует базовому варианту от Microsoft.



Регистрация в системе

После загрузки компьютера и если включена опция “требовать ctrl-alt-del”, на экране появляется приглашение входа в систему. Обратите внимание на приглашение. Если Вы видите надпись “для начала работы вставьте ключ или нажмите Ctrl-Alt-Delete”, значит токен модуль

успешно загружен и готов к работе. Если же надпись гласит “для начала работы нажмите Ctrl-Alt-Delete”, то это означает, что токен-модуль не загружен и вход возможен только вручную - с помощью ввода имени пользователя и пароля.

Возможные причины ошибки загрузки токен-модуля:

- недоступность считывателя в результате физического отключения, сбоя настроек драйверов или PC/SC, наличия неисправности;
- отсутствие в системе DLL файла токен-модуля или дополнительных компонент, необходимых для работы модуля;
- выбор токен-модуля в пользовательских настройках программы ESMART® Access : Administrator, вместо глобальных;
- терминальный сервер : использование несовместимой операционной системы на сервере или клиенте; использование несовместимого типа электронного ключа.
- лицензионные ограничения.

Далее будем рассматривать только работу с электронными ключами.

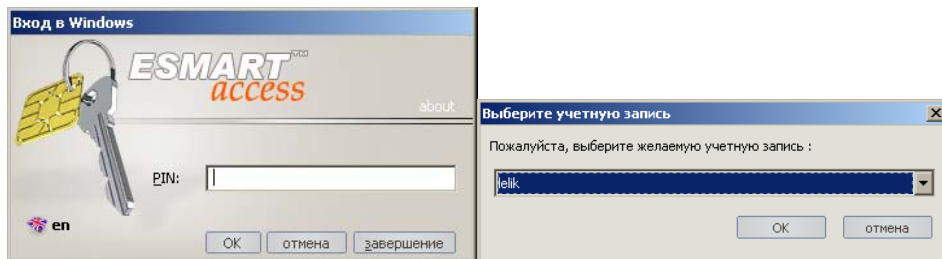
ESMART® Access : GINA отслеживает состояние сразу всех считывателей, поддерживаемых токен-модулем. Например, если у Вас подключено несколько считывателей смарт-карт, то Вы можете вставить карту в любой из них. Далее, до извлечения карты, работа осуществляется только с этим считывателем.

Сразу после загрузки системы проверяется наличие электронного ключа. В том случае, когда он уже вставлен, автоматически начинается процедура входа в систему. Если электронный ключ не вставлен, нужно его вставить. Если процедура входа посредством электронного ключа не начинается, то вытащите его и вставьте его снова. Под словом “вставить” понимается осуществление контакта электронного ключа с компьютером. Это может быть вставление карты в считыватель, ключа в USB порт, поднесение бесконтактной карты к считывателю и любое другое действие, воспринимаемое как подключение электронного ключа к компьютеру. Электронный ключ должен быть предварительно размечен в программе ESMART® Access : Administrator.

Процедура входа в систему зависит от трех факторов:

- Включен ли ПИН код.
- Сколько учетных записей хранится в электронном ключе. Одна или более.
- Если учетных записей более одной, назначена ли запись для авто-входа.

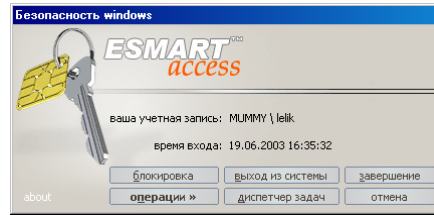
Когда ПИН код включен, система просит его ввести. Если учетных записей более одной и не определена запись для авто-входа, то предлагается выбрать учетную запись из списка.



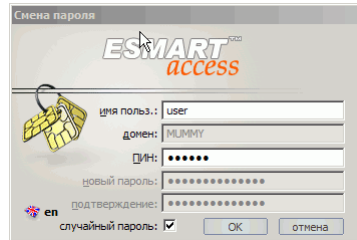
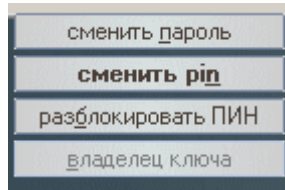
Чтобы сделать вход в систему полностью автоматическим, выключите ПИН код и назначьте, при необходимости, запись для авто-входа. Однако **в целях безопасности отключать ПИН код не рекомендуется!**

Действия пользователя после входа в систему

В процессе работы с компьютером Вы можете нажать Ctrl-Alt-Del, чтобы вызвать диалоговое окно “Безопасность windows”.

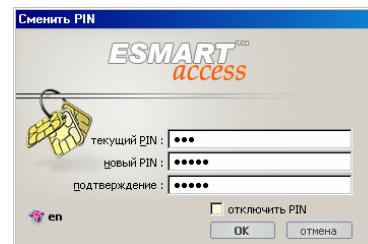


Здесь Вы можете выполнить стандартные операции: заблокировать компьютер, выйти из системы, перезагрузить или выключить компьютер, вызвать диспетчер задач. Дополнительные возможности доступны в выпадающем по кнопке “операции” меню.

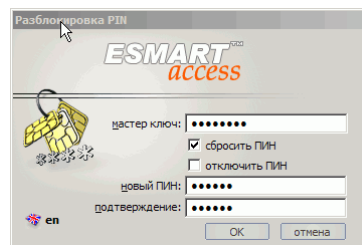


Смена пароля происходит параллельно в системе и электронном ключе. Сначала меняется пароль в системе. В случае успеха новый пароль записывается в электронный ключ. Если в системе пароль изменен успешно и произошла ошибка записи пароля в электронный ключ, то нарушится синхронизация пароля между ключом и системой, и вход станет невозможен. Чтобы устранить проблему, воспользуйтесь ESMART® Access : Administrator.

Для того чтобы поменять или отключить ПИН код, не обязательно пользоваться ESMART® Access : Administrator. Это можно сделать прямо из ESMART® Access : GINA. Введите текущий и два раза новый ПИН код. Чтобы отключить ПИН, введите текущий код и пометьте флажок “отключить ПИН”.

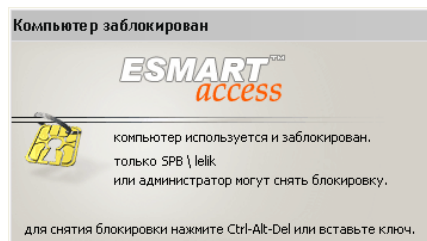


Вы так же можете разблокировать ПИН код, не пользуясь программой ESMART® Access : Administrator. При предъявлении заблокированного кода система автоматически предлагает его разблокировать. Это можно сделать и вручную из меню операций. Для разблокировки ПИН введите Мастер код. Если ПИН код утерян, его можно сбросить на произвольное значение.



Состояние блокировки компьютера

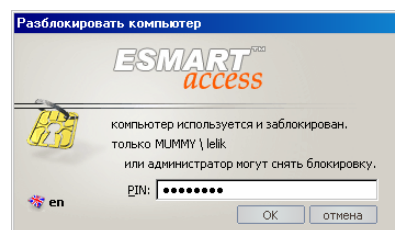
Компьютер может быть заблокирован двумя способами: по желанию пользователя из диалога “безопасность windows” или путем извлечения электронного ключа (только если включена блокировка при извлечении электронного ключа). В этом состоянии выдается следующая заставка (если включена опция “требовать ctrl-alt-del”).



Выхода из состояния блокировки так же два: разблокировка и принудительное завершение сеанса. Чтобы разблокировать компьютер, Вы должны либо предъявить системе пароль текущего пользователя, либо электронный ключ, содержащий этот пароль. Чтобы принудительно завершить сеанс, необходимо предъявить учетную запись другого пользователя, обладающего правами администратора на данном компьютере. В последнем случае несохраненные данные текущего пользователя теряются.

Для разблокировки посредством электронного ключа Вы должны его вставить. Процесс разблокировки напоминает вход в систему и зависит от следующих факторов:

- Включен ли ПИН код.
- Сколько учетных записей хранится в памяти электронного ключа : одна или более.
- Если учетных записей более одной, назначена ли запись для авто-входа.
- Каким способом был заблокирован компьютер: вручную или при извлечении электронного ключа;
- Включено ли требование Ctrl-Alt-Del.



Автоматическая разблокировка достигается при соблюдении следующего условия:

<ПИН код выключен> И
(<Количество учетных записей = 1> ИЛИ <Выбрана запись для авто-входа>) И
(<Компьютер заблокирован при извлечении электронного ключа> ИЛИ
<Включено требование Ctrl-Alt-Del>)

Последняя группа условий позволяет избежать разблокирования компьютера сразу же после его ручного блокирования.

Раздел 5. Особенности различных электронных ключей

В настоящем разделе дается представление о том, как реализована работа с каждым типом электронных ключей. Хотя почти всегда различия прозрачны для пользователя, понимание принципов работы токен-модулей необходимо, чтобы правильно оценить все риски, связанные с использованием тех или иных электронных ключей и выбрать для себя наиболее подходящий тип.

Таблица совместимости ОС и различных электронных ключей

При локальном использовании	Вид электронного ключа		2000	XP	2003
		Смарт-карты	✓	✓	✓
		Aladdin eToken	✓	✓	✓
		Карты ESMART® Access Lite	✓	✓	✓
		USB-Drive	✓	✓	✓

При использовании терминальной сессии	Вид электронного ключа		2000*	XP*	2003*
		Смарт-карты		✓	✓
		Aladdin eToken		✓	✓
		Карты ESMART® Access Lite			
		USB-Drive			

* В таблице указаны версии ОС сервера. ОС клиента должна быть Windows 2000,XP,2003,Vista.

1. ESMART® Access card.

ESMART® Access card является базовой картой для использования в системах ESMART® Access. Карта полностью аппаратно реализует все возможности системы. Объем памяти карты – 8 Кб.

2. Карты Schlumberger Cryptoflex.

Карты Cryptoflex применяются в тех случаях, когда требуется совместное использование карт в системе ESMART® Access и приложениях PKI (например, для безопасной электронной переписки в Microsoft Outlook). Поддерживаются карты следующих типов:

- Cryptoflex for Windows® 2000;
- Cryptoflex for Windows® XP;
- Cryptoflex 8K;
- Cryptoflex 16K.

Несмотря на свое название, Cryptoflex for Windows® 2000/XP по сути являются Cryptoflex 8K. Отличие состоит лишь в начальном форматировании карты производителем,

которое все равно уничтожается при форматировании карты в ESMART® Access. Поддерживаются следующие шаблоны форматирования:

- ESMART® Access only. Все свободное пространство отдается приложению. Карта не будет работать с PKI.
- Cryptoflex for Windows® 2000 + ESMART® Access.
- Cryptoflex for Windows® XP + ESMART® Access.

Два последних формата полностью идентичны оригинальным картам от Schlumberger, за исключением создания специфических для ESMART® Access структур данных, которые никак не влияют на работу карты с PKI.

При использовании карт в PKI нельзя делать ПИН код пустым или отключать его. Это несовместимо с крипто-провайдером от Schlumberger.

Карты Cryptoflex полностью аппаратно реализуют все возможности системы.

3. Aladdin eToken PRO

eToken PRO подключается напрямую к USB порту компьютера и базируется на интегрированной в корпус токена смарт-карте, оснащенной операционной системой CardOS/M4. Токен поддерживает все возможности ESMART® Access, кроме одной тонкости. ПИН код не может быть разблокирован без его смены.

eToken PRO обладает собственным криптопроцессором, позволяющим эффективно и безопасно использовать его в приложениях PKI. Объем памяти составляет 16, 32 или 64 Кб.

Доступ к устройствам eToken осуществляется через стандартный интерфейс смарт-карт PC/SC. После установки Aladdin RTE, в системе создаются виртуальные считыватели смарт-карт, называемые “AKS ifdh N” (N=0,1). Когда пользователь вставляет электронный ключ, система думает, что вставляется смарт-карта в один из виртуальных считывателей. Как правило, первый вставленный токен видится через считыватель “AKS ifdh 0”.

4. USB drive

USB drive является общедоступным и широко используемым устройством flash памяти большого объема – от 32 Мб до 4Гб и более. USB drive не содержит никаких средств защиты данных. Все функции реализуются программной эмуляцией. Данные приложения хранятся в скрытом каталоге в корне диска. Файлы шифруются уникальной для каждого диска информацией и не могут быть просто переписаны на другой носитель.

USB drive представляет собой устройство с однофакторной аутентификацией. Из всех поддерживаемых устройств оно является наименее защищенным.

5. Карты ESMART® Access Lite

Данные карты являются картами памяти объемом 256 байт. Для использования карт требуется считыватель смарт-карт компании ACS: ACR30S (COM порт), ACR30U (USB) или ACR38 (USB). Доступ к картам памяти реализуется через нестандартную (proprietary) библиотеку, не совместимую с PC/SC. По этой причине считыватель не может быть одновременно задействован в PC/SC приложениях. Ввиду некоторых особенностей реализации proprietary библиотеки рекомендуется отказаться от устройств чтения ACR30S, т.к. при их использовании резко возрастает загрузка процессора (до 25% на устройство). Чтобы обеспечить параллельный доступ к считывателям из нескольких процессов, устанавливается менеджер ресурсов, выполненный в виде сервиса SLEMgr.

Сами карты памяти не содержат каких-либо средств защиты данных, которые могли бы быть использованы в ESMART® Access. Чтение карты возможно всегда. Т.е., при раскрытии

алгоритмов шифрования, пароли с карты могут быть восстановлены без знания каких-либо кодов.

Небольшой объем памяти не дает возможности хранить записную книжку и информацию менеджера паролей на карте. На карту вмещается только служебная информация и одна запись для входа в систему. Как опция, реализовано хранение данных на жестком диске компьютера. В этом случае с карты читается только уникальный ID код, и становится возможным использование менеджера паролей и записной книжки.

Раздел 6. Удаление ESMART® Access

Удаление программы производится стандартными средствами Windows® – через сервис «Установка и удаление программ» из Панели Управления Windows. Производится удаление программы ESMART® Access.