JaCarta SecurLogon

Руководство администратора

Версия: 1.1

Редакция от: 24 ноября 2015 г.

Листов: 32

Аннотация

Данное Руководство администратора (далее – Руководство) предназначено для персонала, осуществляющего установку, эксплуатацию и настройку программного обеспечения (ПО) JaCarta SecurLogon.

В настоящем Руководстве приведены общие сведения, системные требования, режимы работы, порядок и содержание действий по установке лицензии, созданию, редактированию и удалению профилей и изменению настроек административного шаблона ПО JaCarta SecurLogon.

Руководство рассчитано на пользователей, обладающих начальными навыками работы на компьютере, знакомых с работой в операционной системе Windows и Интернет.

Содержание

1. Общие сведения

JaCarta SecurLogon работает в составе ПО Единый клиент JaCarta. ПО JaCarta SecurLogon функционально представляет собой отдельный программный продукт, однако физически является расширением функциональности бесплатного ПО Единый Клиент JaCarta. То есть ПО JaCarta SecurLogon по умолчанию устанавливается при установке ПО Единый клиент JaCarta, но пользователь сможет им воспользоваться лишь после того, как будет приобретена и установлена лицензия на ПО JaCarta SecurLogon.

JaCarta SecurLogon позволяет повысить уровень безопасности при входе на локальный компьютер и в корпоративную сеть под управлением ОС Windows за счёт простого и быстрого перехода от авторизации по логину и паролю к двухфакторной аутентификации на основе электронного ключа. При этом отсутствует необходимость настройки Active Directory, внедрения PKI-инфраструктуры и создания собственного Удостоверяющего центра для выпуска сертификатов пользователей. При использовании JaCarta SecurLogon конечный пользователь не будет вводить с клавиатуры пароль Windows, что исключает возможность подсматривания или перехвата пароля злоумышленником.

1.1. Назначение

JaCarta SecurLogon предназначено для двухфакторной аутентификации пользователя при входе в ОС Microsoft Windows или в сетевой домен с использованием электронного ключа (токена).

JaCarta SecurLogon обеспечивает:

1) двухфакторную аутентификацию с использованием профиля пользователя, хранящегося в электронном ключе JaCarta/eToken, для получения доступа к локальному ПК или к сетевым ресурсам;

2) управление профилем[1)] пользователя с последующей записью профиля на безопасное хранение в память электронного ключа (токена) JaCarta/eToken;

3) хранение одного или нескольких профилей пользователя на одном электронном ключе JaCarta/eToken;

4) генерацию случайных паролей пользователя;

5) синхронизацию с локальным или доменным паролем пользователя;

6) средства администрирования-настройки для:

- определения параметров безопасности, ограничений и реакции системы на отсоединение электронного ключа JaCarta/eToken;

- управления полномочиями пользователей;

7) блокировку компьютера при отсутствии пользователя.

[1)] *Профиль - набор данных, включающий имя пользователя, домен, к которому принадлежит данный пользователь/имя компьютера, и пароль.*

1.2. Возможности

1) Возможность выбора следующих методов аутентификации с помощью токенов и смарт-карт JaCarta/eToken на локальном (не подключенном к сети) компьютере и в домене Windows:

- вход по логину\паролю, вводимому с клавиатуры;
- вход по сертификату, хранимому на токене/смарт-карте;
- вход по профилю JaCarta SecurLogon, в котором сохранён пароль, введённый вручную;
- вход по профилю JaCarta SecurLogon, в котором сохранён случайно сгенерированный пароль.

2) Возможность каждые X дней автоматически менять пароль пользователя на новый – только для случая, если пользователь использует метод аутентификации по профилю JaCarta SecurLogon со случайно сгенерированным паролем.

3) Возможность блокировки компьютера пользователя сразу после извлечения USB-токена или смарт-карты.

4) Возможность использования уникальных биометрических характеристик (отпечаток пальца) для входа в ОС Microsoft Windows, в домен или для доступа к сетевым информационным ресурсам.

5) Возможность использования цифровых сертификатов для входа в домен и на локальный компьютер при развёртывании инфраструктуры PKI.

Если в памяти токена имеется сертификат пользователя и соответствующий закрытый ключ, их можно использовать для входа в домен Windows вместо имени пользователя и пароля.

1.3. Дополнительная документация

Для полного понимания настоящего документа рекомендуется ознакомиться с документом [Единый клиент JaCarta. Руководство администратора], содержащим сведения, касающиеся системных требований, установки и настройки Единого клиента JaCarta, а также сведения, касающиеся работы с электронными ключами.

2. Системные требования

2.1. Требования к программному обеспечению

JaCarta SecurLogon может применяться со следующими операционными системами, установленными на ПК пользователя:

- Windows Vista SP2 (32- или 64-бит);
- Windows 7 (32- или 64-бит);
- Windows 8 (32- или 64-бит);
- Windows 8.1 (32- или 64-бит);
- Windows 10 (32- или 64-бит);
- Windows Server 2008 R2;
- Windows Server 2008 (32- или 64-бит);
- Windows Server 2012 (64-бит);
- Windows Server 2012 R2.

На ПК пользователя также должно быть установлено следующее программное обеспечение:

- драйвер устройства чтения смарт-карт (при необходимости);
- Единый клиент JaCarta.

2.2. Применяемые модели электронных ключей JaCarta/eToken

JaCarta SecurLogon может применяться со следующими моделями электронных ключей:

- JaCarta PKI, PKI/Flash;
- JaCarta ГОСТ, JaCarta ГОСТ/Flash;
- JaCarta PKI/ГОСТ, PKI/ГОСТ/Flash;
- JaCarta PKI/BIO, JaCarta PKI/BIO/ГОСТ;
- JaCarta LT;
- eToken PRO, eToken PRO (Java);
- eToken NG-Flash.

2.3. Требования к аппаратному обеспечению

Конфигурация ПК пользователя JaCarta SecurLogon должна удовлетворять требованиям, изложенным в документации операционной системы.

Для установки Единый клиент JaCarta требуется не менее 125 Мбайт дискового пространства.

Для работы с USB-ключом JaCarta/eToken требуется минимум один свободный порт USB.

Для работы со смарт-картой требуется устройство чтения смарт-карт (например, ASEDrive).

3. Подготовка к работе

3.1. Установка

ПО JaCarta SecurLogon по умолчанию устанавливается при установке ПО Единый клиент JaCarta. Порядок установки и удаления ПО Единый клиент JaCarta описан в документе [Единый клиент JaCarta. Руководство администратора].

3.2. Смена PIN-кода электронного ключа

Внимание! При получении электронного ключа на руки настоятельно рекомендуется осуществить смену PIN-кода пользователя.

После установки ПО Единый клиент JaCarta пользователь имеет возможность сменить PIN-код электронного ключа двумя способами:

1. До входа в ОС с помощью запуска модуля "Управление токеном" (см. рис. 1).
2. После входа в ОС с помощью запуска ПО Единый клиент JaCarta (см. рис. 2).

Для смены PIN-кода необходимо знать текущий PIN-код электронного ключа. Значения PIN-кодов, используемых для различных моделей электронных ключей по умолчанию, приведены в Приложении А (см. таблицу А.2.).

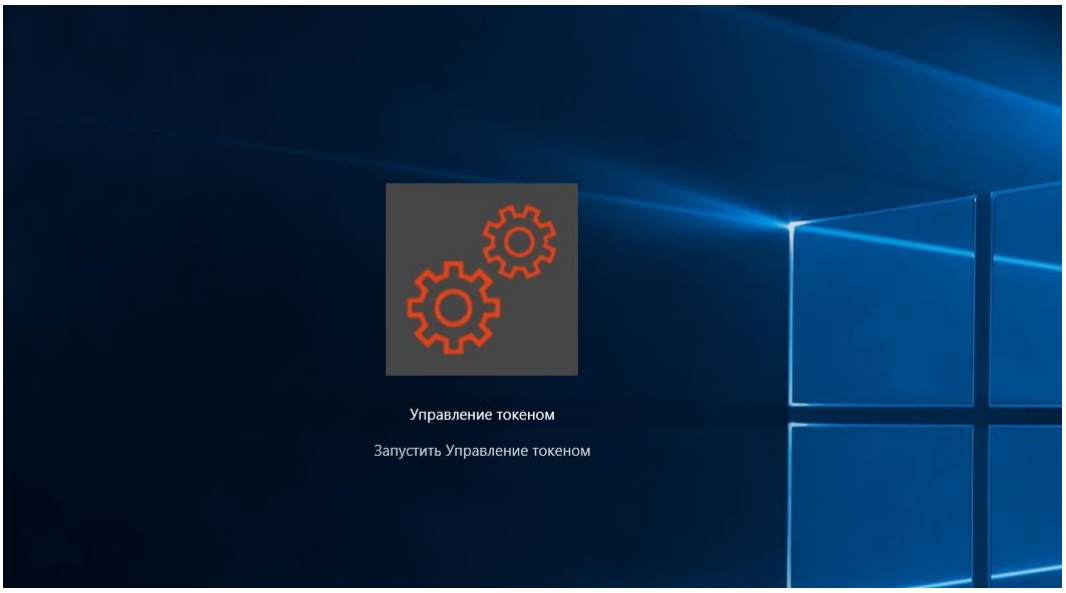


Рисунок 1

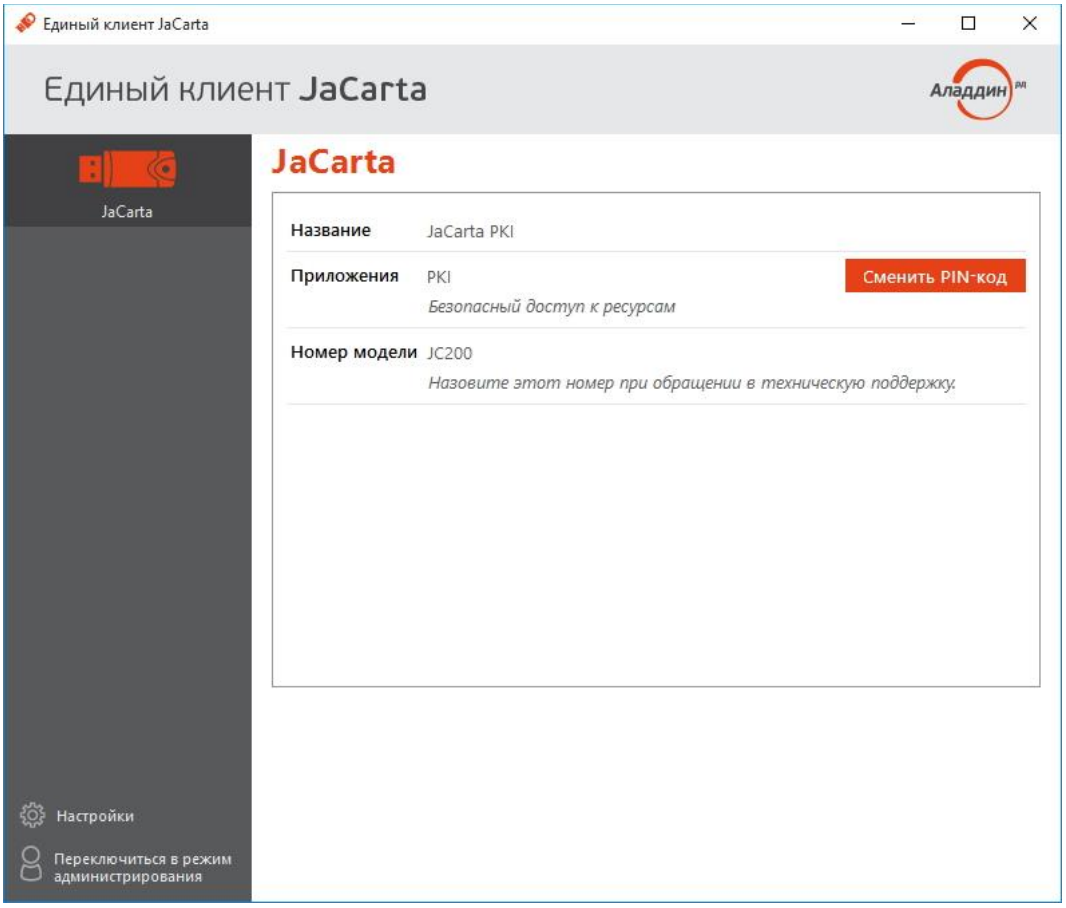


Рисунок 2

После нажатия кнопки "**Сменить PIN-код**" должно появиться окно, показанное на рисунке 3, в котором необходимо ввести текущий PIN-код, новый PIN-код и подтвердить PIN-код, введя его еще раз.

Если все данные введены правильно, то после нажатия кнопки "**Выполнить**" должно появиться окно, показанное на рисунке 4.

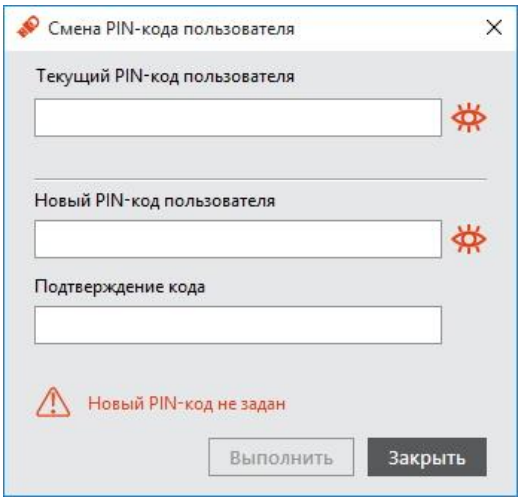


Рисунок 3

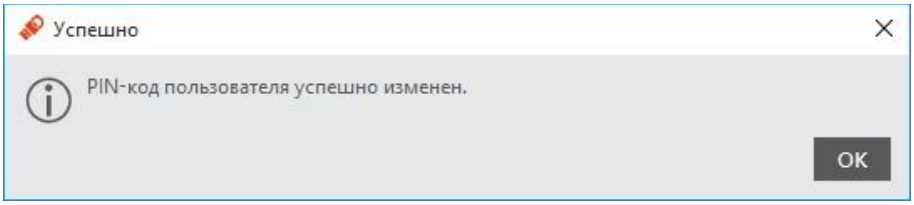


Рисунок 4

3.3. Режимы работы

Единый клиент JaCarta может работать в двух режимах:

1. Режим пользователя – позволяет просматривать краткие сведения о подсоединённых электронных ключах и предоставляет доступ к базовым операциям с электронными ключами.
2. Режим администрирования – позволяет просматривать полные сведения о подсоединённых электронных ключах и предоставляет доступ ко всем операциям с электронными ключами.

Для переключения в режим администрирования необходимо в окне Единого клиента JaCarta кликнуть левой кнопкой мыши по надписи "**Переключиться в режим администрирования**" (см. рис. 5).

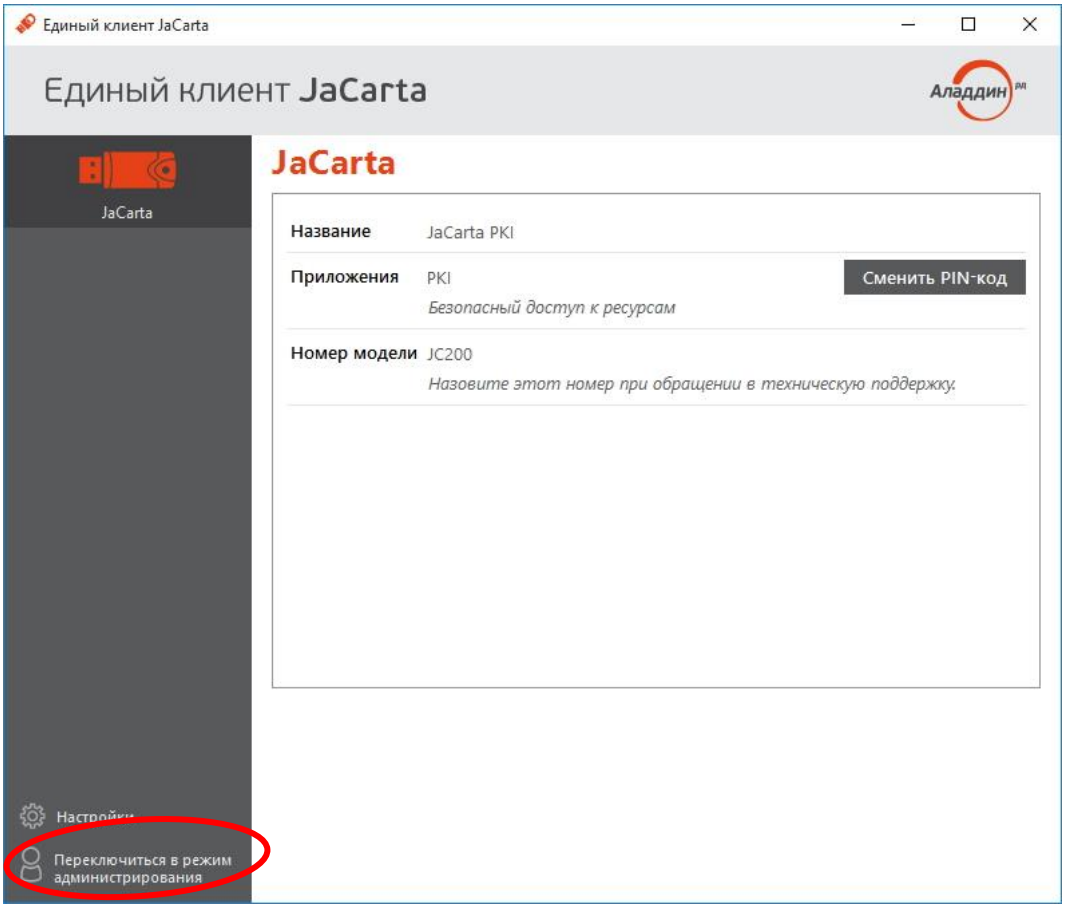


Рисунок 5

Для переключения в режим пользователя необходимо в окне Единого клиента JaCarta кликнуть левой кнопкой мыши по надписи "**Переключиться в режим пользователя**" (см. рис. 6).

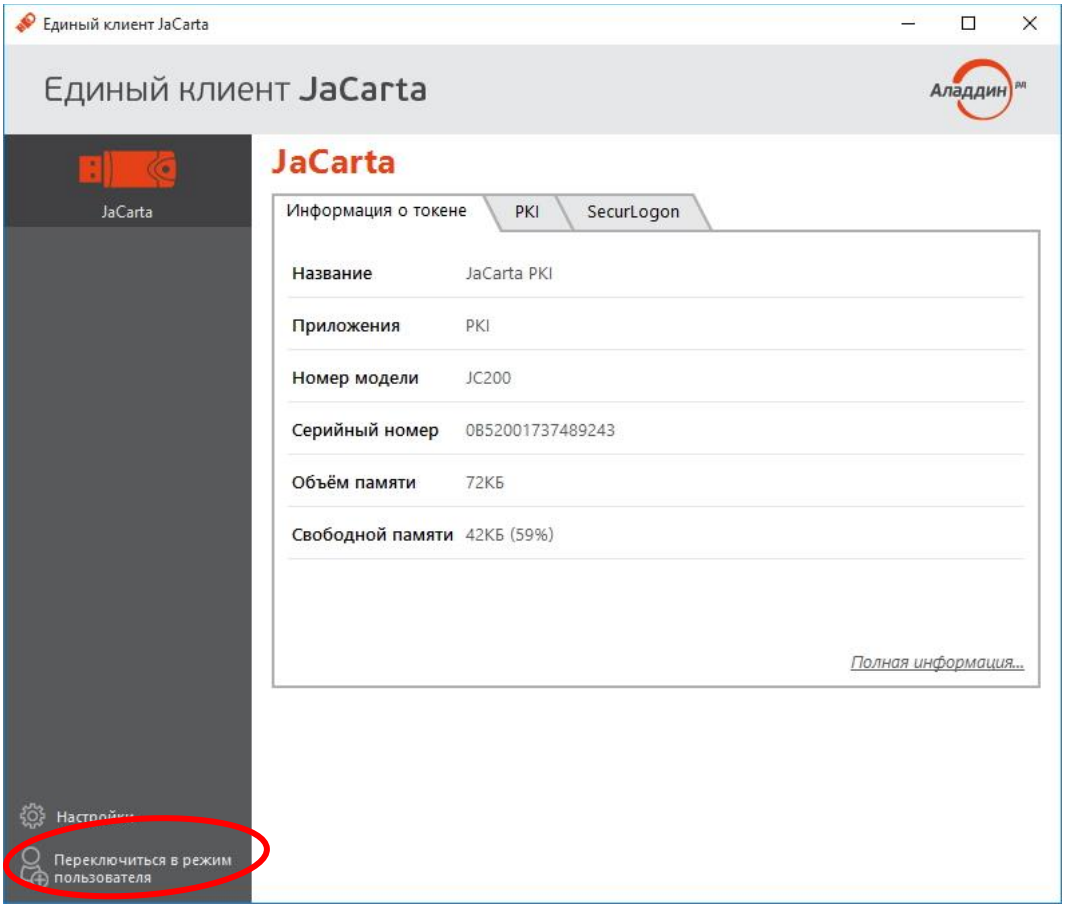


Рисунок 6

3.4. Установка лицензии

Установить лицензию JaCarta SecurLogon можно двумя способами:

1. В режиме пользователя: через меню Настройки в окне Единого клиента JaCarta;
2. В режиме администрирования: через вкладку SecurLogon в окне Единого клиента JaCarta.

Чтобы установить лицензию, необходимо обладать правами администратора.

В случае установки лицензии через вкладку SecurLogon в окне Единого клиента JaCarta необходимо подсоединить электронный ключ к компьютеру.

В случае установки лицензии через меню Настройки в окне Единого клиента JaCarta подсоединять электронный ключ к компьютеру не обязательно.

3.4.1. Установка лицензии через меню Настройки

Установку лицензии через меню Настройки производить в следующей последовательности:

1. Запустить Единый клиент JaCarta и кликнуть левой кнопкой мыши по надписи **Настройки** в левом нижнем углу окна Единого клиента JaCarta (см. рис. 7.).

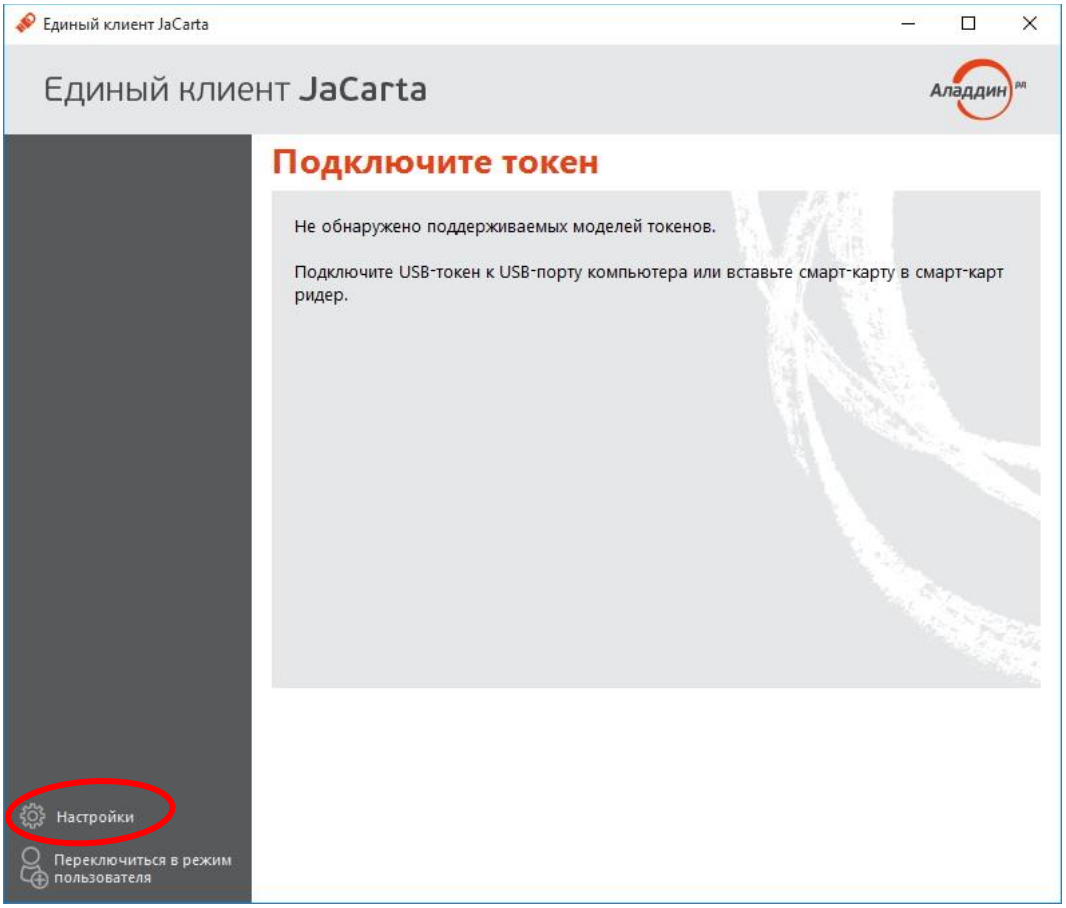


Рисунок 7

2. В отобразившемся окне выбрать вкладку SecurLogon и нажать кнопку "**Установить лицензию SecurLogon…**" (см. рис.8).

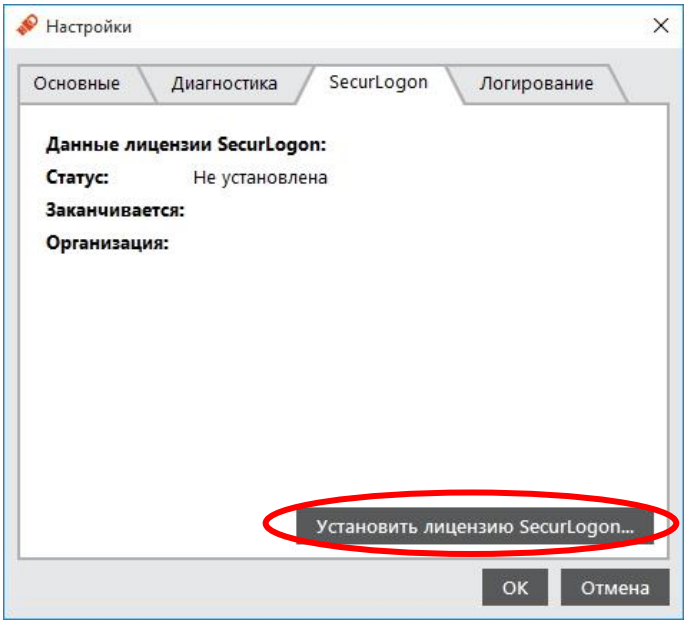


Рисунок 8

3. В отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку "**Открыть**".
4. После установки лицензии в отобразившемся окне нажать кнопку **ОК** (см. рис. 9).

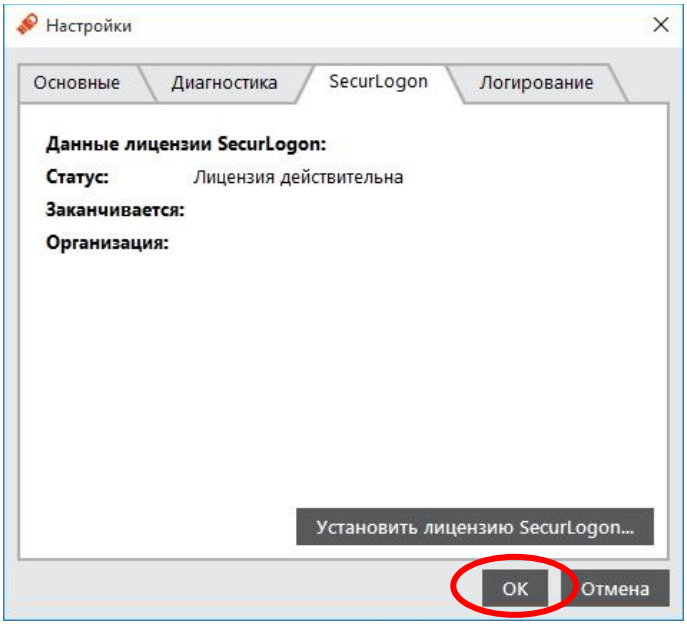


Рисунок 9

3.4.2. Установка лицензии через вкладку SecurLogon

Установку лицензии через вкладку SecurLogon производить в следующей последовательности:

1. Подключить электронный ключ к компьютеру и запустить Единый клиент JaCarta, после чего переключиться в режим администратора, перейти на вкладку SecurLogon и в статусе лицензии нажать ссылку "установить" (см. рис. 10.).

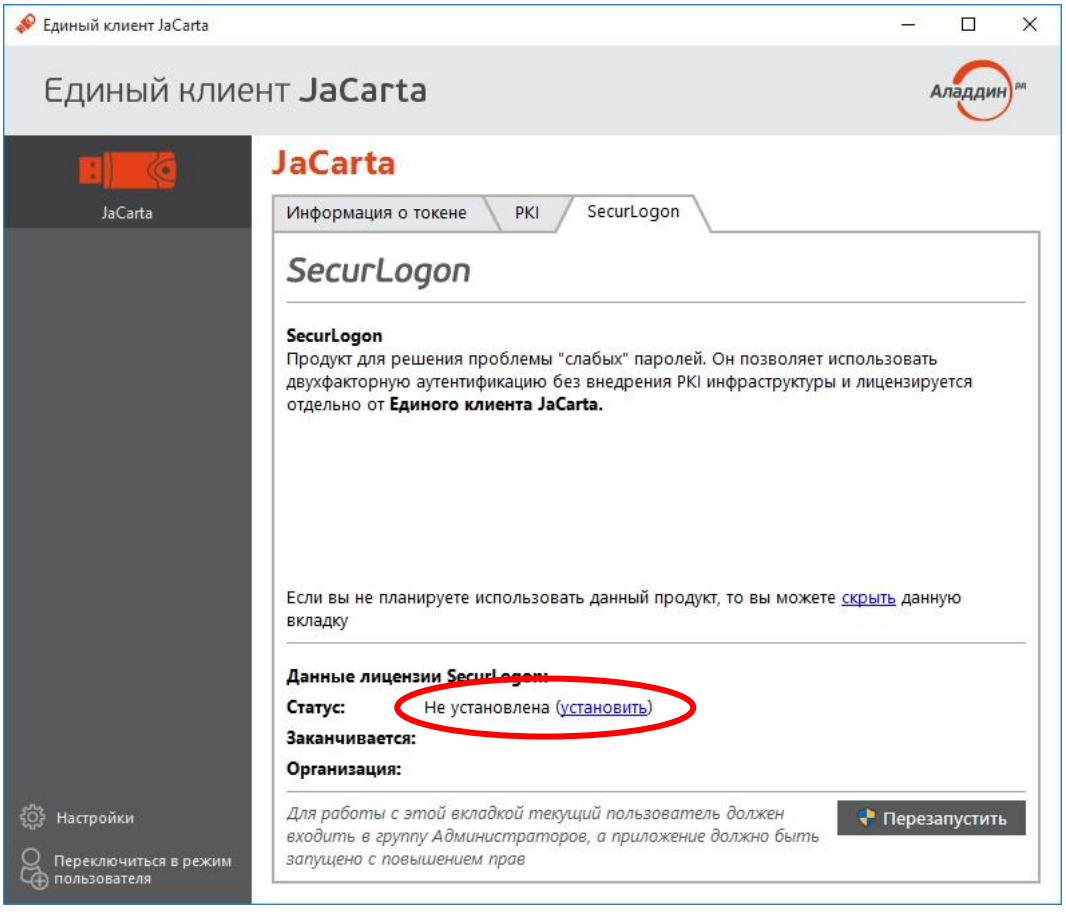


Рисунок 10

2. Далее в отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку "**Открыть**".
3. При успешном завершении операции вкладка SecurLogon примет следующий вид (см. рис.11).

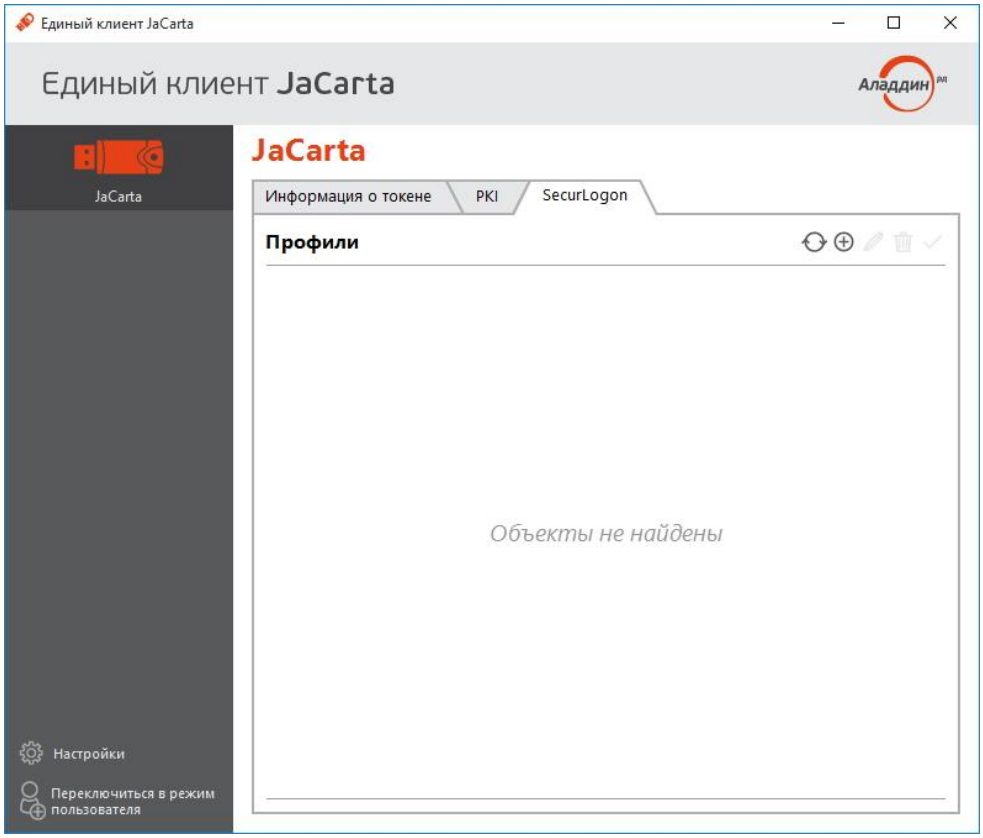


Рисунок 11

4. Настройка работы

4.1. Операции с профилями

4.1.1. Создание профиля JaCarta SecurLogon

Чтобы создать профиль JaCarta SecurLogon, необходимо выполнить следующие действия:

1. Подсоединить электронный ключ, на котором требуется создать профиль JaCarta SecurLogon, к компьютеру и запустить Единый клиент JaCarta;
2. Переключиться в режим администратора и перейти на вкладку SecurLogon;

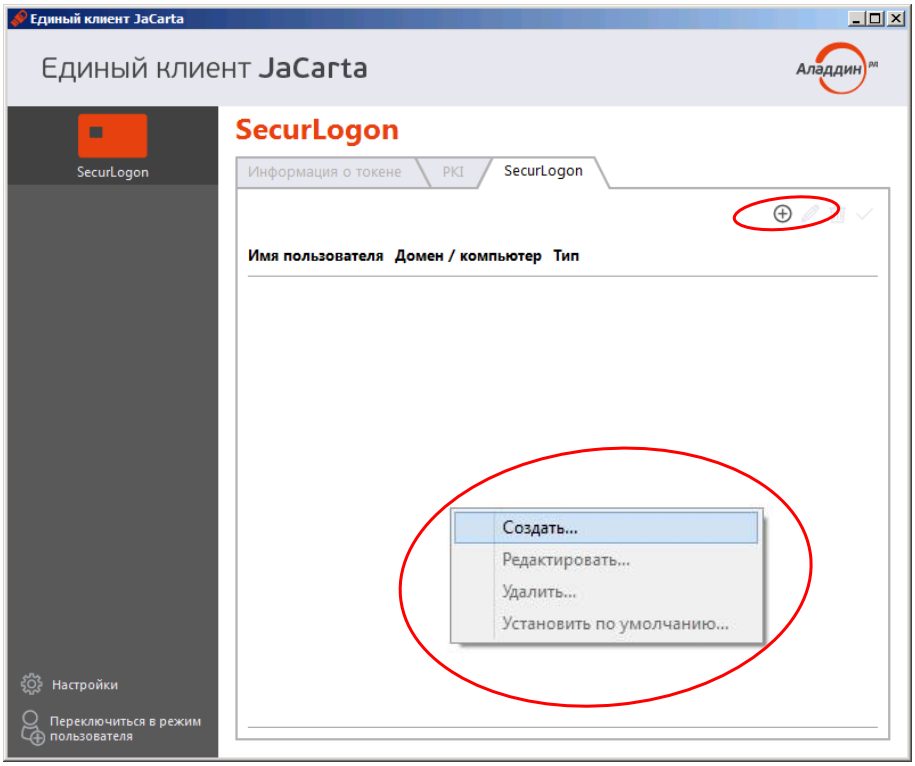


Рисунок 12

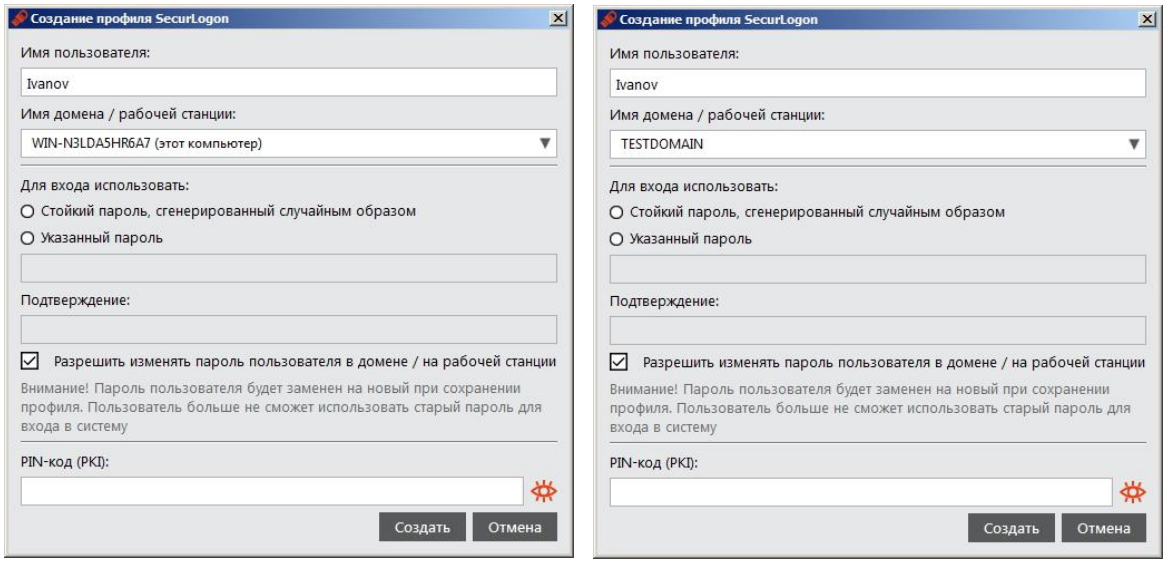
3. Нажать на значок ⊕ или нажать правой кнопкой мыши в центральной части окна и в контекстном меню выбрать "**Создать…**" (см. рис. 12);

В зависимости от того, создаётся ли профиль JaCarta SecurLogon для локальной учётной записи или для учётной записи в домене Windows окно создания профиля может быть двух видов (см. рис. 13 а) – для локальной учетной записи и рис. 13 б) – для учетной записи в домене Windows).

4. В появившемся окне (см. рис. 13) следует выбрать, какой тип пароля будет использоваться для входа, ввести PIN-код электронного ключа и нажать кнопку "**Создать**";

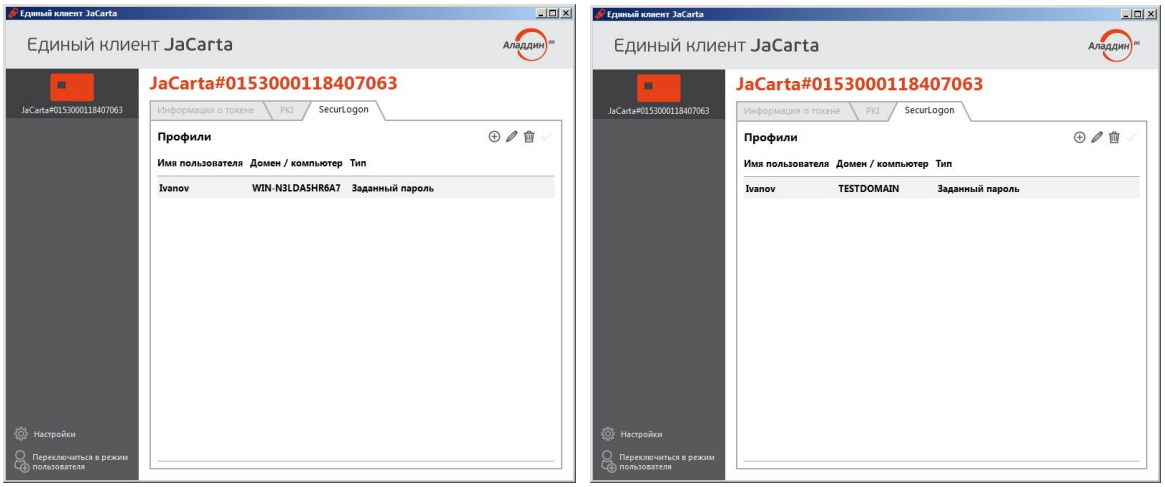
Подробная информация о выборе типа пароля и других настройках при создании профиля JaCarta SecurLogon представлена в таблице 1.

5. Созданный профиль должен отобразиться в окне Единого клиента JaCarta на вкладке SecurLogon (см. рис. 14 а) – для локальной учетной записи и б) – для учетной записи в домене Windows).



а) б)

Рисунок 13



а) б)

Рисунок 14

Таблица 1 Атрибуты профиля JaCarta SecurLogon

Название настройки	Описание настройки	
	Рабочая станция	Домен
Имя пользователя	Задает имя пользователя, для которого будет создаваться профиль SecurLogon. Редактирование поля с данной настройкой может быть недоступно, если в административном шаблоне JaCarta SecurLogon отключена настройка **CanCreateProfilesForOtherUsers** (Создание профилей для других пользователей).	
Имя домена / рабочей станции	Позволяет выбрать или имя домена или имя рабочей станции (место, где хранится учётная запись пользователя). Соответственно, если выбрано имя рабочей станции (имя компьютера), то профиль JaCarta SecurLogon будет создан для локальной учётной записи, а если выбрано имя домена, то профиль JaCarta SecurLogon будет создан для учётной записи, находящейся в домене Windows.	

<table>
<tr><th rowspan="2">Название настройки</th><th colspan="2">Описание настройки</th></tr>
<tr><th>Рабочая станция</th><th>Домен</th></tr>
<tr><td>Для входа использовать</td><td colspan="2">Позволяет выбрать один из двух пунктов:
Стойкий пароль, сгенерированный случайным образом – пароль для учётной записи пользователя будет сгенерирован случайным образом;
Указанный пароль – пароль для учётной записи будет введён вручную; при выборе этого пункта становятся активными два поля:
поле для ввода пароля;
поле Подтверждение, в котором нужно указать подтверждение введённого пароля.  Пользователь, который создаёт профиль JaCarta SecurLogon (администратор SecurLogon), должен обладать достаточными правами для смены пароля пользователя, для которого создаётся профиль SecurLogon (пользователь JaCarta SecurLogon).</td></tr>
<tr><td>Имя пользователя для домена</td><td>Не актуально</td><td>Позволяет ввести имя пользователя учётной записи домена (администратора JaCarta SecurLogon)
  Настройка активна, только если установлен флажок Разрешить изменять пароль пользователя в домене / на рабочей станции (подробнее см. описание соответствующей настройки ниже).</td></tr>
<tr><td>Пароль для домена</td><td>Не актуально</td><td>Позволяет ввести пароль для учётной записи домена (администратора JaCarta SecurLogon)
  Настройка активна, только если установлен флажок Разрешить изменять пароль пользователя в домене / на рабочей станции (подробнее см. описание соответствующей настройки ниже).</td></tr>
<tr><td>Разрешить изменять пароль пользователя в домене / на рабочей станции</td><td colspan="2">Данная настройка определяет, будет ли изменён пароль учётной записи пользователя, для которого создаётся профиль JaCarta SecurLogon.

Если флажок установлен, то будет установлен пароль, заданный в настройке Для входа использовать: (т.е. это может быть случайный пароль или пароль, введённый администратором при создании профиля). При этом администратор JaCarta SecurLogon, который создаёт профиль JaCarta SecurLogon, должен обладать достаточными полномочиями для смены пароля учётной записи пользователя JaCarta SecurLogon.

При создании профиля JaCarta SecurLogon для учётной записи в домене Windows также необходимо заполнить следующие поля:
Имя пользователя для домена;
Пароль для домена.
В этих полях необходимо указать имя пользователя и пароль учётной записи администратора JaCarta SecurLogon, который впоследствии сможет изменять пароль пользователя JaCarta SecurLogon.</td></tr>
<tr><td>PIN-код</td><td colspan="2">Позволяет ввести текущий PIN-код электронного ключа</td></tr>
</table>

Таблица 1

 Если в настройках административного шаблона JaCarta SecurLogon параметр **AllowProfileManagement** отключен, то создание профилей будет заблокировано.

 Если на электронном ключе уже есть профиль текущего пользователя, а в настройках административного шаблона JaCarta SecurLogon параметр **SingleProfileOnly** отключен, то создание других профилей будет заблокировано.

 Если в настройках административного шаблона JaCarta SecurLogon параметр **CanCreateProfilesForOtherUsers** отключен, то при создании нового профиля изменение имени текущего пользователя будет заблокировано.

4.1.2. Установка профиля по умолчанию

JaCarta SecurLogon позволяет установить профиль по умолчанию – т.е. такой профиль будет отображаться первым при входе в систему.

Чтобы установить профиль по умолчанию, необходимо выполнить следующие действия:

1. Подсоединить электронный ключ, на котором находится профиль JaCarta SecurLogon, к компьютеру.
2. Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.
3. Левой кнопкой мыши выбрать профиль, который необходимо сделать профилем по умолчанию.
4. В окне Единого клиента JaCarta нажать на значке ✓ (см. рис. 15) или нажать правой кнопкой мыши на строке с выбранным профилем и из контекстного меню выбрать "**Установить по умолчанию…**".

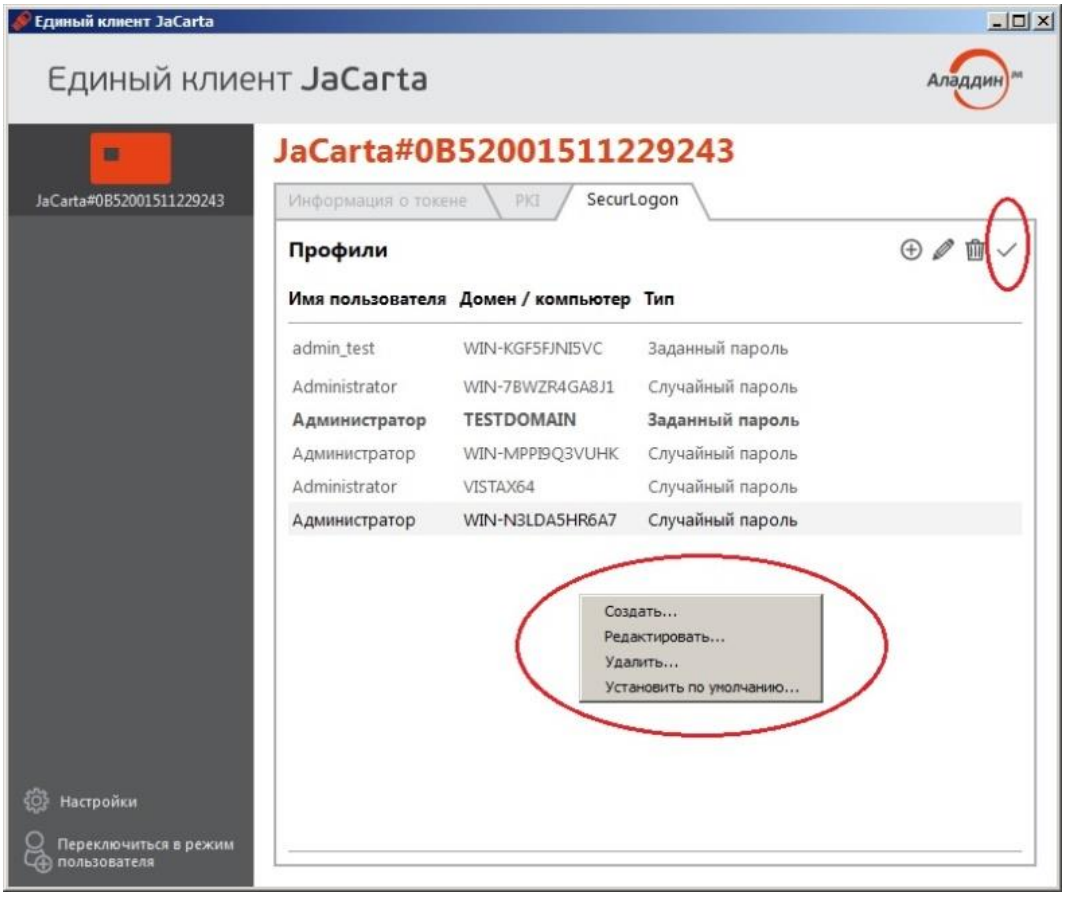


Рисунок 15

5. Далее в отобразившемся окне (см. рис. 16) ввести PIN-код и нажать **ОК**.

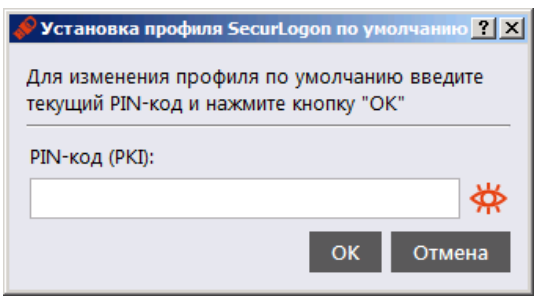


Рисунок 16

6. Выбранный ранее профиль в окне Единого клиента JaCarta должен стать профилем по умолчанию, т.е. быть выделен жирным шрифтом среди других профилей (см. рис. 17).

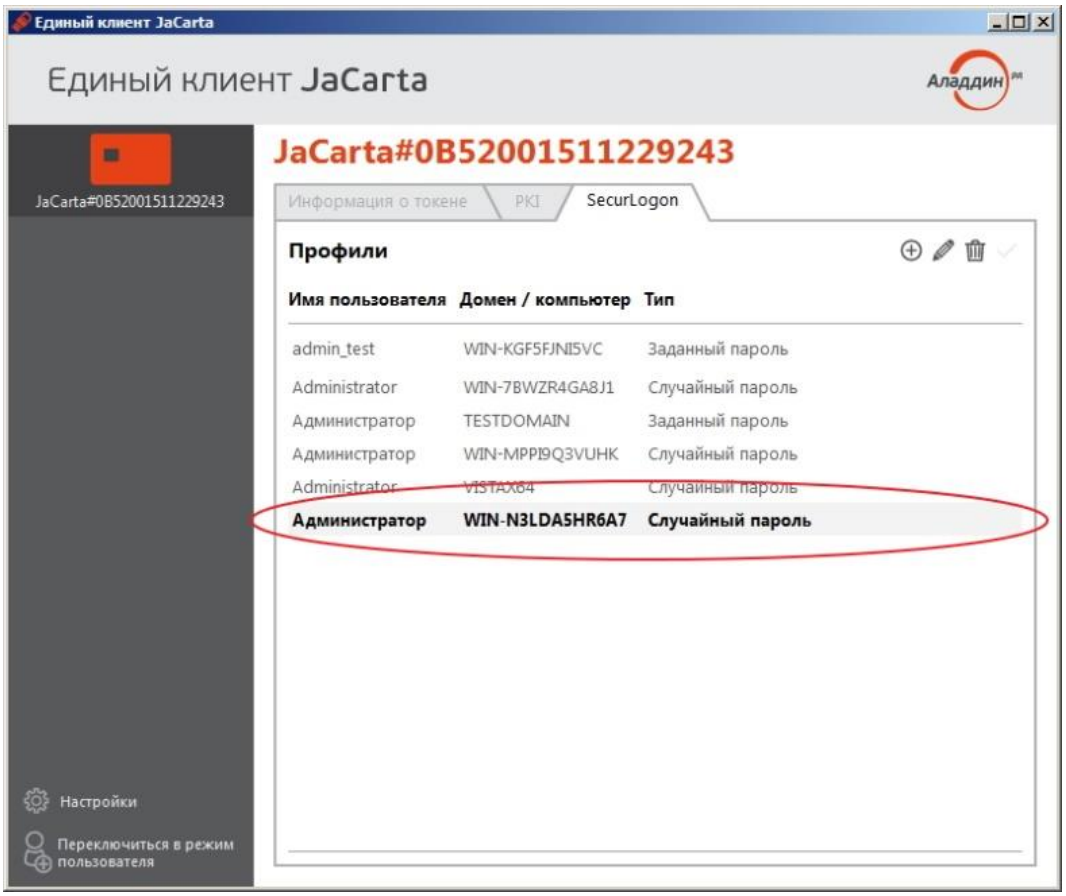


Рисунок 17

4.1.3. Редактирование существующего профиля

Чтобы отредактировать профиль JaCarta SecurLogon, необходимо выполнить следующие действия:

1. Подсоединить электронный ключ с записанным профилем JaCarta SecurLogon к компьютеру.
2. Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.
3. Левой кнопки мыши выбрать профиль, который необходимо изменить.
4. Нажать на значок (см. рис. 18) или нажать правой кнопкой мыши на выбранном профиле и из контекстного меню выбрать "**Редактировать…**".

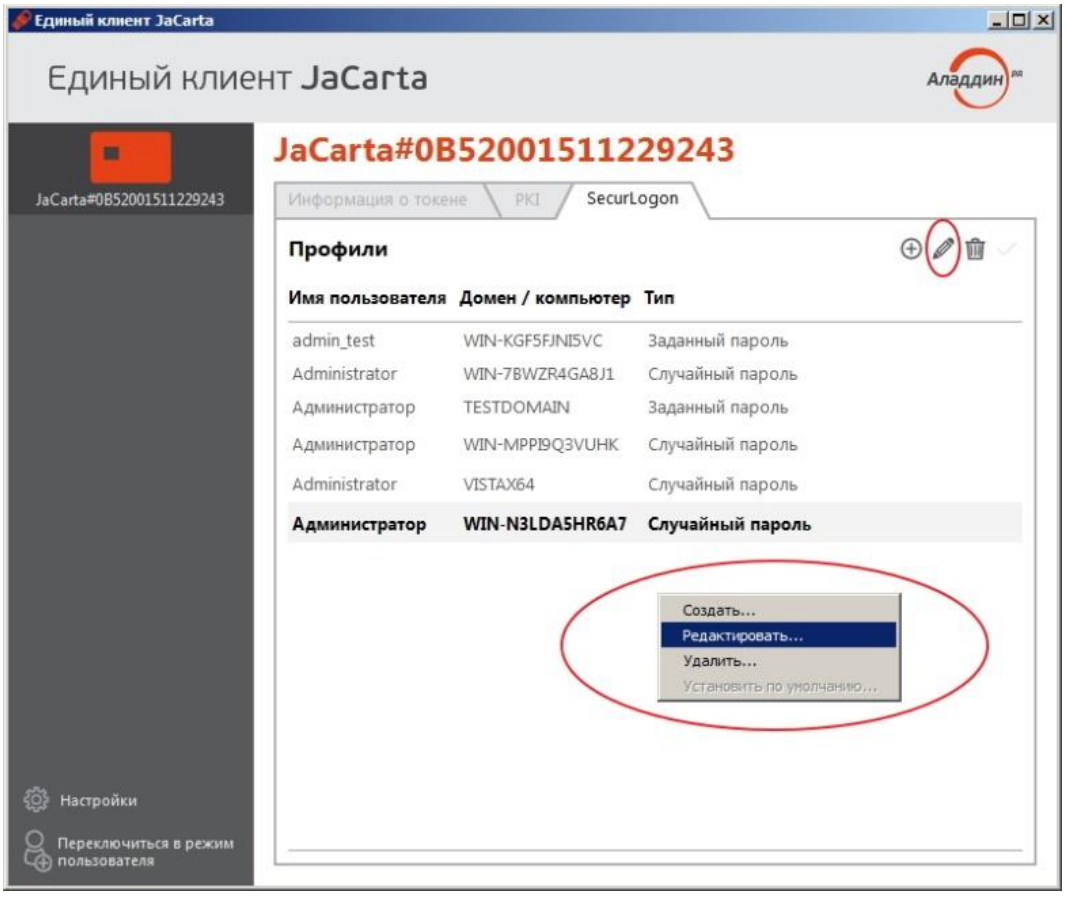


Рисунок 18

5. Далее в отобразившемся окне (см. рис. 19) выполнить необходимые изменения и нажать "**Сохранить**".

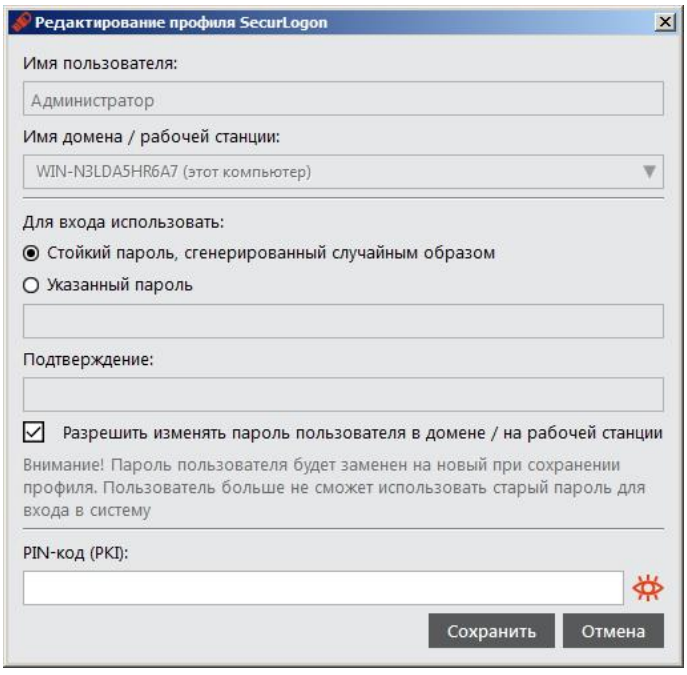


Рисунок 19

4.1.4. Удаление профиля

Чтобы удалить профиль JaCarta SecurLogon из памяти электронного ключа, необходимо выполнить следующие действия:

1. Подсоединить электронный ключ с записанным профилем JaCarta SecurLogon к компьютеру.
2. Запустить Единый клиент JaCarta, переключиться в режим администратора и перейти на вкладку SecurLogon.
3. Нажатием левой кнопки мыши выбрать профиль, который необходимо удалить.
4. Нажать на значок или нажать правой кнопкой мыши на выбранном профиле и из контекстного меню выбрать "**Удалить…**" (см. рис. 20).

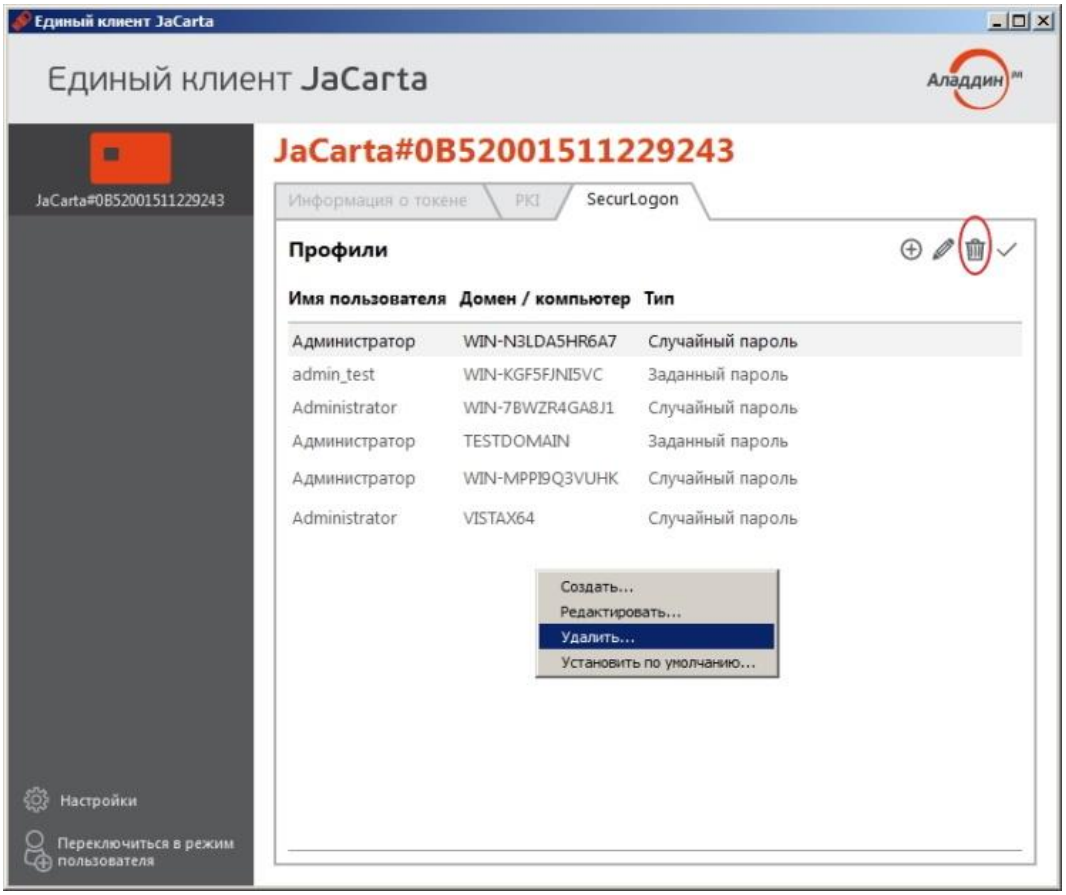


Рисунок 20

Дальнейшая процедура различается в зависимости от типа пароля, установленного при создании профиля JaCarta SecurLogon (указанный пароль (вводимый вручную) или стойкий пароль, сгенерированный случайным образом).

В случае, если при создании профиля был выбран "Указанный пароль", то в отобразившемся окне следует ввести PIN-код электронного ключа и нажать кнопку "**Удалить**" (см. рис. 21).

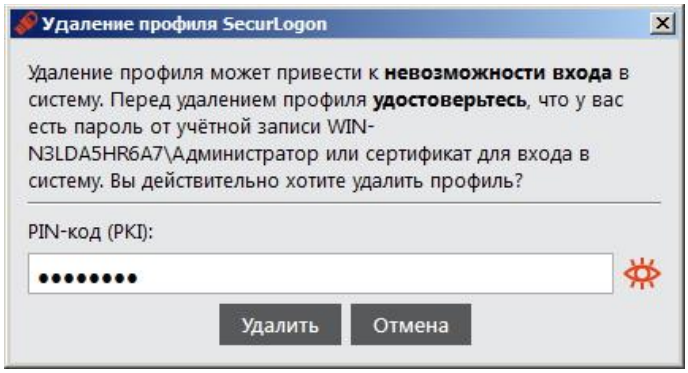


Рисунок 21

В случае, если при создании профиля был выбран "Стойкий пароль, сгенерированный случайным образом", то в отобразившемся окне следует ввести новый пароль (пароль, который будет назначен учетной записи пользователя после удаления профиля JaCarta SecurLogon) и повторно подтвердить введенный пароль, после чего ввести PIN-код электронного ключа и нажать кнопку "**Удалить**" (см. рис. 22).

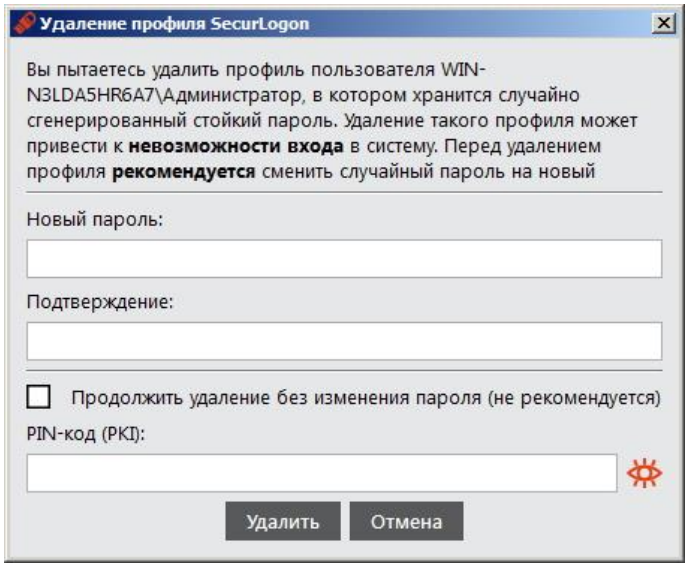


Рисунок 22

Если установить флажок в опции "Продолжить удаление без изменения пароля (не рекомендуется)", то вводить новый пароль и его подтверждение не требуется, однако, после удаления профиля JaCarta SecurLogon для доступа к учётной записи пользователя сохранится случайный пароль, сгенерированный при создании профиля JaCarta SecurLogon.

Внимание! Не рекомендуется устанавливать этот флажок, т.к. в этом случае пароль для доступа к учётной записи пользователя останется неизвестным, а доступ будет невозможен.

4.2. Настройка административного шаблона

4.2.1. Настройка административного шаблона для групповых политик при работе с сервера

Перечисленные ниже действия следует выполнять на сервере, являющимся контроллером домена или и на компьютере, на которым установлены средства управлениям контроллером домена.

Чтобы запустить административный шаблон JaCarta SecurLogon и отобразить его настройки необходимо выполнить следующие действия:

1. Нажать на клавиатуре сочетание клавиш **Win+R**, в появившемся окне набрать **gpmc.msc** и нажать **ОК** (см. рис. 23).

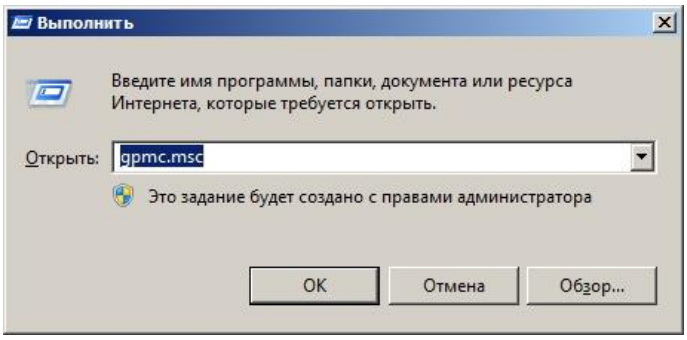


Рисунок 23

2. В появившемся окне (см. рис. 24) следует выбрать **Лес => Домены => имя_домена**, далее нажать правой кнопкой мыши на пункте **Default Domain Policy** (Политика домена по умолчанию) и из появившегося контекстного меню выбрать опцию "**Изменить…**".

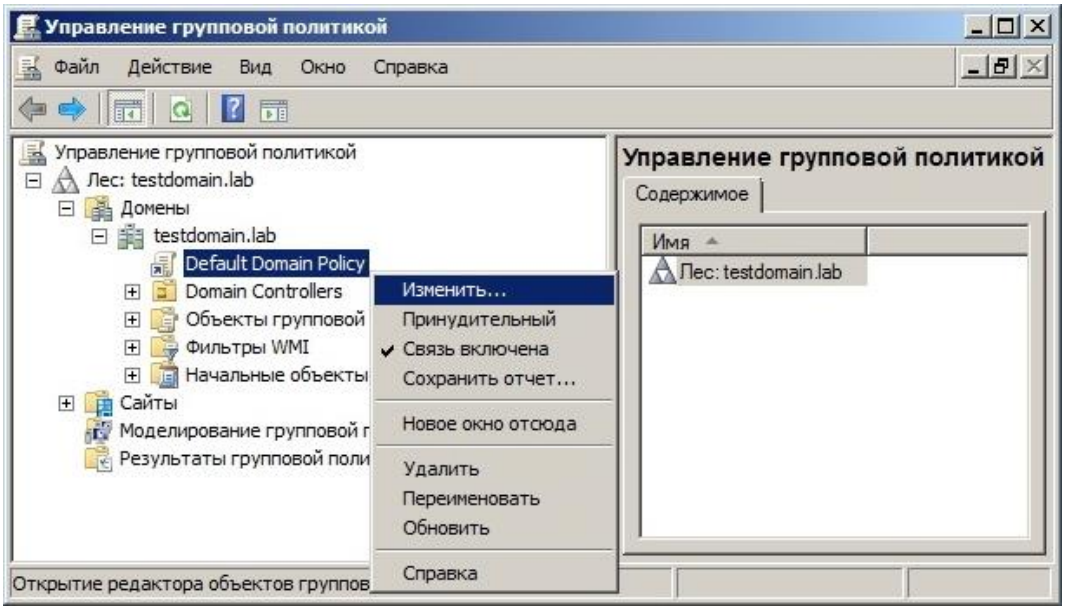


Рисунок 24

3. В появившемся окне (см. рис. 25) следует выбрать **Конфигурация компьютера => Политики => Административные шаблоны => JaCarta SecurLogon**.

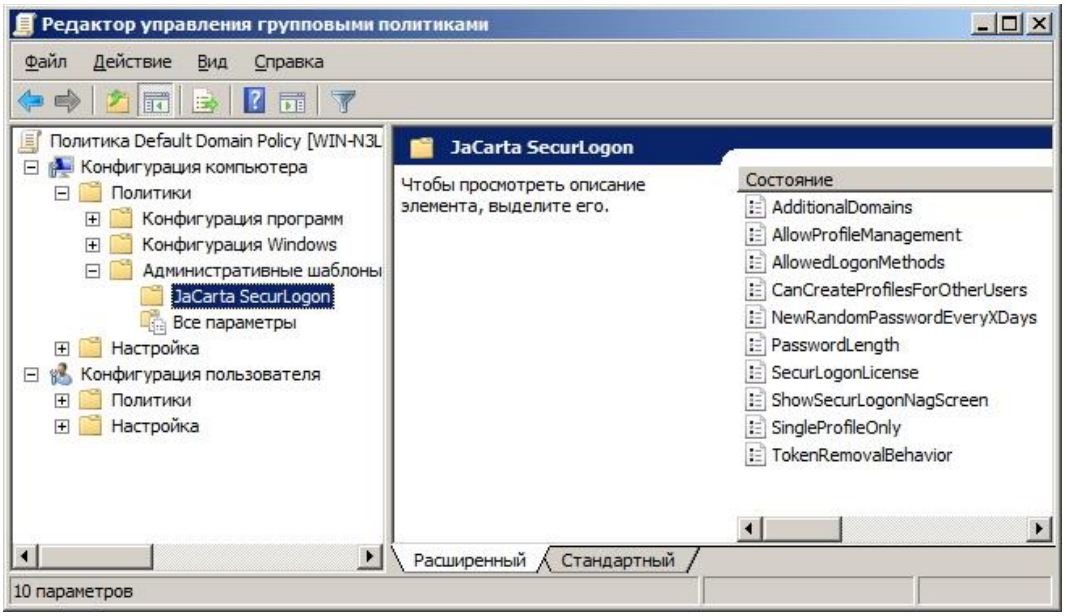


Рисунок 25

4. Редактирование административного шаблона JaCarta SecurLogon производится путем изменения значения параметров политик, входящих в шаблон.

Описание настроек административного шаблона JaCarta SecurLogon с указанием значений параметров политик по умолчанию приведены в Приложении А.

4.2.2. Настройка административного шаблона для групповых политик при работе с локального ПК

4.2.2.1. Запуск шаблона

Чтобы запустить административный шаблон JaCarta SecurLogon и отобразить его настройки необходимо выполнить следующие действия:

1. Нажать на клавиатуре сочетание клавиш **Win+R**, в появившемся окне набрать **gpedit.msc** и нажать **ОК** (см. рис. 26).

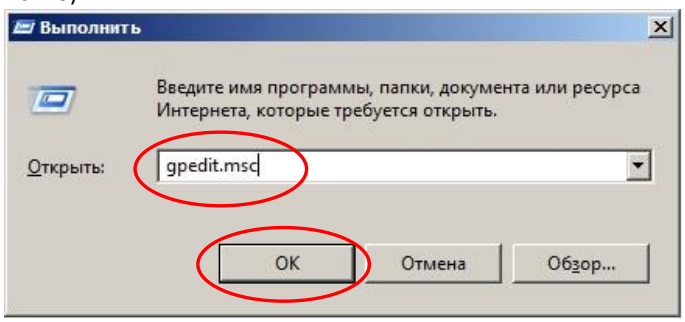


Рисунок 26

2. В появившемся окне выбрать **Конфигурация компьютера => Административные шаблоны => Компоненты Windows => JaCarta SecurLogon** (см. рис. 27).

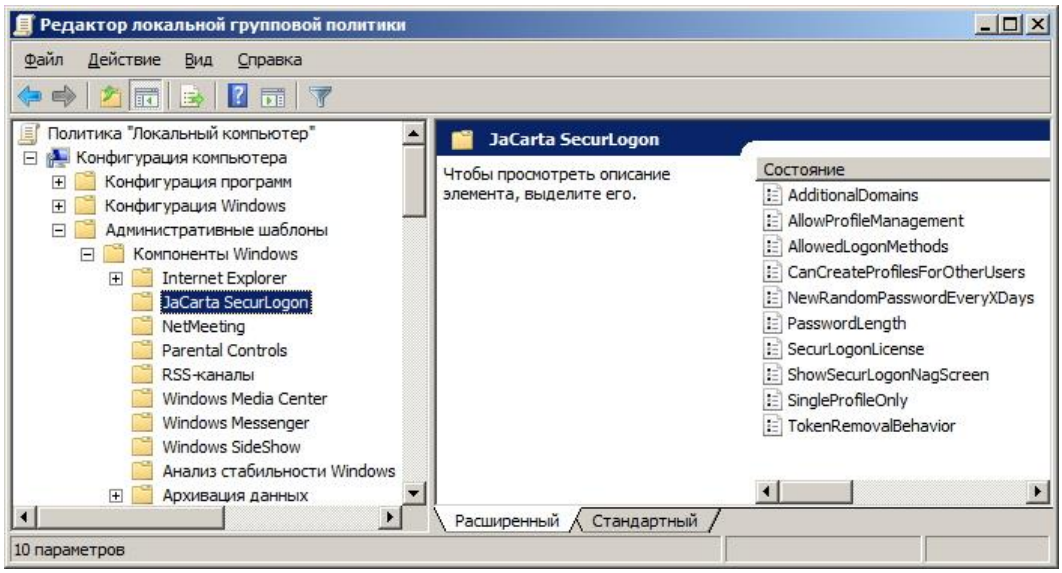


Рисунок 27

3. Редактирование административного шаблона JaCarta SecurLogon производится путем изменения значения параметров политик, входящих в шаблон.

Описание настроек административного шаблона JaCarta SecurLogon с указанием значений параметров политик по умолчанию приведены в Приложении А.1.

4.3. Разблокировка электронного ключа

В случае, если пользователь введет несколько раз подряд неправильный PIN-код, то его электронный ключ будет заблокирован.

Для разблокировки электронного ключа необходимо выполнить действия согласно документу [Единый клиент JaCarta. Руководство администратора].

Приложение А

Настройки административного шаблона JaCarta SecurLogon

Таблица А.1.

Название параметра	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[2)]	Значение по умолчанию в шаблоне[3)]
AdditionalDomains (Дополнительные домены)	Список дополнительных доменов, отображаемых при создании профиля или при входе с использованием профиля SecurLogon.	**Имена доменов Windows**, указанные через точку с запятой ИЛИ **пустая строка**.	Пустая строка	Пустая строка
AllowProfileManagement (Разрешить создание профилей пользователями)	Разрешает или запрещает пользователям создавать профили SecurLogon	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – пользователи могут самостоятельно создавать профили; **Отключено** – пользователи не могут самостоятельно создавать профили.	Включено	Отключено
AllowedLogonMethods (Разрешённые методы аутентификации)	Определяет перечень доступных методов аутентификации, которые доступны для входа в операционную систему.	**Не задано** – будет использоваться значение по умолчанию (последний столбец настоящей таблицы); **Отключено** – будут использоваться стандартные механизмы Windows; **Включено** – позволяет явно задать, какие методы входа можно будет использовать (при этом значение 1 означает, что метод разрешён, а 0 – запрещён): **DefaultPasswordLogon** – стандартный вход в систему с использованием имени пользователя и пароля, вводимых с клавиатуры; **DefaultSmartCardLogon** – вход с использованием сертификата, хранящегося в памяти электронного ключа; **ManualPasswordLogon** – пароль для профиля SecurLogon вводится вручную; **RandomPasswordLogon** – для профиля SecurLogon генерируется случайный пароль.	Выбраны все методы	Выбраны все методы

[2)] *Эти значение применяются сразу после установки Единого клиента JaCarta*

[3)] *Применяются после распространения групповых политик, если в административный шаблон SecurLogon не было внесено никаких изменений*

Название параметра	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[2)]	Значение по умолчанию в шаблоне[3)]
CanCreateProfilesForOtherUsers (Создание профилей для других пользователей)	Разрешает или запрещает пользователю создавать профили для других пользователей.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – пользователь может создавать профили для других учетных записей; **Отключено** – пользователь может создавать профили только для текущей учетной записи.	Включено	Отключено
NewRandomPasswordEveryXDays (Автоматически менять пароль каждые X дней)	Обновление случайного пароля для профиля SecurLogon каждые X дней. (Пользователь при этом должен запоминать только PIN-код электронного ключа.)	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – при выборе этого пункта становится активным соответствующее поле, в котором нужно указать период (в днях), по истечении которого пароль для учётной записи Windows будет меняться; **Отключено** – пароль учётной записи Windows не будет меняться автоматически.	Отключено	Отключено
PasswordLength (Длина случайного пароля учётной записи)	Задаёт длину случайного пароля для профиля SecurLogon.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – при выборе этого пункта становится активным соответствующее поле, в котором нужно указать длину случайного пароля (в символах), допустимые значения – от 14 до 63 символов; **Отключено** – настройка не применяется.	63	63
SecurLogonLicense (Лицензия SecurLogon)	Строка, содержащая лицензию SecurLogon.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – при выборе этого пункта становится активным соответствующее поле, в которое необходимо полностью скопировать содержимое файла лицензии (для этого фай лицензии можно открыть в текстовом редакторе); **Отключено** – лицензия не устанавливается (пустая строка);	Пустая строка	Пустая строка
ShowSecurLogonNagScreen (Отображать вкладку SecurLogon, если лицензия не установлена)	Определяет отображать или не отображать вкладку SecurLogon, если лицензия не установлена.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – вкладка отображается; **Отключено** – вкладка не отображается.	Включено	Включено

Название параметра	Описание	Допустимые значения	Значение по умолчанию до распространения групповых политик[2)]	Значение по умолчанию в шаблоне[3)]
SingleProfileOnly (Один профиль на электронном ключе)	Разрешает или запрещает создание на одном электронном ключе нескольких профилей SecurLogon.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Включено** – пользователи могут создать только один профиль на электронном ключе; **Отключено** – пользователи могут создавать несколько профилей на одном электронном ключе.	Отключено	Отключено
TokenRemovalBehavior (Поведение при отсоединении электронного ключа от компьютера)	Данная настройка определяет поведение системы в ситуации, в которой пользователь, осуществивший вход с помощью профиля SecurLogon, отсоединяет электронный ключ от компьютера.	**Не задано** – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); **Отключено** – никакие действия предприниматься не будут; **Включено** – при выборе этого пункта становится активным соответствующий список, в котором можно выбрать вариант поведения системы: **Не выполнять никаких действий** – при отсоединении электронного ключа не предпринимается никаких действий; **Блокировать рабочую станцию** – при отсоединении электронного ключа происходит блокировка рабочего стола; **Принудительный выход из системы** – при отсоединении электронного ключа производится принудительный выход из системы пользователя; **Отключение при подключении через RDP** – при отсоединении электронного ключа происходит разрывания сеанса подключения через удалённый рабочий стол.	Не выполнять никаких действий	Не выполнять никаких действий

Таблица А.1.

Значения PIN-кодов по умолчанию

Таблица А.2.

Параметры	Модели электронных ключей:				
	eToken PRO eToken PRO (Java) eToken NG-FLASH eToken NG-FLASH (Java) eToken NG-OTP eToken NG-OTP (Java) JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin.	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO	JaCarta ГОСТ/Flash JaCarta ГОСТ eToken ГОСТ	JaCarta LT	JaCarta CryptoPro
Приложение	PKI	PKI и PKI/BIO	ГОСТ	STORAGE	ФКН
PIN-код пользователя по умолчанию	1234567890	11111111	Не установлен	1234567890	Нет
Поведение ключа при разблокировке PIN-кода пользователя[4]	Во время разблокировки администратор задаёт новый PIN-код пользователя		Разблокировка сбрасывает счётчик неверных попыток доступа – PIN-код пользователя при этом остаётся неизменным		Нет
Можно разблокировать PIN-код пользователя в удалённом режиме	Да	Да	Нет	Нет	Нет
Администратор может сменить установленный PIN-код пользователя без инициализации	Да	Да	Нет	Нет	Нет

Таблица А.2.

[4] *В случае с электронными ключами JaCarta PKI/BIO при разблокировке биометрического доступа пользователь вновь получает возможность аутентифицироваться по ранее сохранённому отпечатку пальца.*

Сокращения и аббревиатуры

ГОСТ	Государственный стандарт
ОС	Операционная система
ПО	Программное обеспечение
ПК	Персональный компьютер
PIN	(Personal Identification Number) личный опознавательный номер
PKI	(Public Key Infrastructure) инфраструктура открытых ключей
USB	(Universal Serial Bus) универсальная последовательная шина

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения
1.1	Внесены изменения в разделы 1, 2, 3.
1.0	*Создание документа*

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00073 от 20.08.13
Microsoft Silver OEM Hardware Partner, Apple Developer, Oracle Gold Partner

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru