Средство аутентификации и безопасного хранения информации пользователей JaCarta

JaCarta SecurLogon

Руководство администратора для Microsoft Windows

Обозначение документа	RU.АЛДЕ.03.01.019-01 32 02
Статус	Публичный
Листов	33

Оглавление

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 Microsoft Windows.

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 ПО Единый Клиент JaCarta. Установка ПО JaCarta SecurLogon происходит с помощью дистрибутива Единого Клиента 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 Microsoft 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 для входа в ОС Microsoft 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:

- двухфакторную аутентификацию с использованием профиля пользователя, хранящегося в электронном ключе JaCarta/eToken, для получения доступа к локальному ПК или к сетевым ресурсам;
- управление профилем[1] пользователя с последующей записью профиля на безопасное хранение в память электронного ключа (токена) JaCarta/eToken;
- хранение одного или нескольких профилей пользователя на одном электронном ключе JaCarta/eToken;
- генерацию случайных паролей пользователя;
- синхронизацию с локальным или доменным паролем пользователя;
- возможности администрирования и настройки для:
  - определения параметров безопасности, ограничений и реакции системы на отсоединение электронного ключа JaCarta/eToken;
  - управления полномочиями пользователей.
- блокировку компьютера при отсутствии пользователя.

1.2 Возможности

- Возможность выбора следующих методов аутентификации с помощью электронных ключей 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 электронном ключе/смарт-карте;
  - вход по профилю JaCarta SecurLogon, в котором сохранён пароль, введённый вручную;
  - вход по профилю JaCarta SecurLogon, в котором сохранён случайно сгенерированный пароль.
- 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;
- Возможность блокировки компьютера пользователя сразу после извлечения электронного ключа или смарт-карты;

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

- Возможность использования уникальных биометрических характеристик (отпечаток пальца) для входа в ОС Microsoft Windows, в домен или для доступа к сетевым информационным ресурсам;
- Возможность использования цифровых сертификатов для входа в домен и на локальный компьютер при развёртывании инфраструктуры PKI.

Если в памяти электронного ключа 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 для Windows], 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:

- Microsoft Windows 7 SP1 (32/64-бит)
- Microsoft Windows 8.1 Update 1 (32/64-бит)
- Microsoft Windows 10 (32/64-бит)
- Microsoft Windows Server 2008 SP2 (32/64-бит)
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

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:

Электронные ключи eToken:

- eToken PRO Anywhere;
- eToken NG-OTP (Java);

Электронные ключи JaCarta:

- JaCarta Remote Access;
- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/BIO;
- JaCarta SF/ГОСТ;
- JaCarta PRO;
- JaCarta-2 ГОСТ;
- JaCarta-2 PKI/ГОСТ;
- JaCarta-2 PKI/ГОСТ/Flash;
- JaCarta-2 PRO/ГОСТ;
- JaCarta-2 PKI/BIO/ГОСТ;
- JaCarta-2 SE;
- JaCarta-2 SF;
- Aladdin LiveOffice;
- Aladdin LiveOffice Common Edition;
- JaCarta LT;
- JaCarta WebPass;
- JaCarta U2F;

- JaCarta U2F/WebPass.

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 150 Мбайт дискового пространства.

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

Для работы со смарт-картой требуется устройство чтения смарт-карт.

3. Подготовка к работе

3.1 Установка

ПО JaCarta SecurLogon устанавливается при установке ПО Единый Клиент JaCarta. Порядок установки и удаления ПО Единый Клиент JaCarta описан в документе [Единый Клиент JaCarta. Руководство администратора для Windows].

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. Рисунок 1);

   ИЛИ

2. После входа в ОС с помощью запуска ПО Единый Клиент JaCarta (см. Рисунок 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.

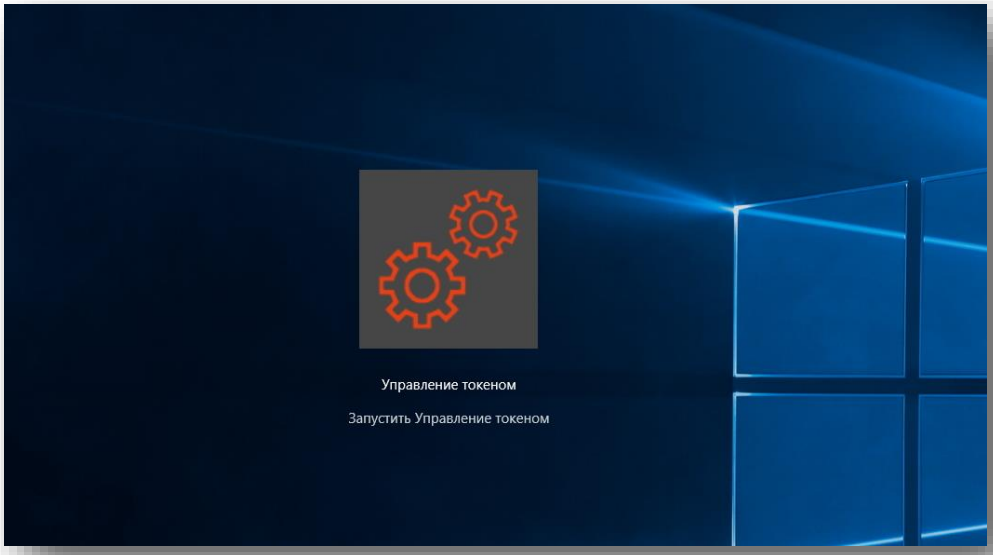

Рисунок 1 – Вход с помощью модуля [Управление токеном]

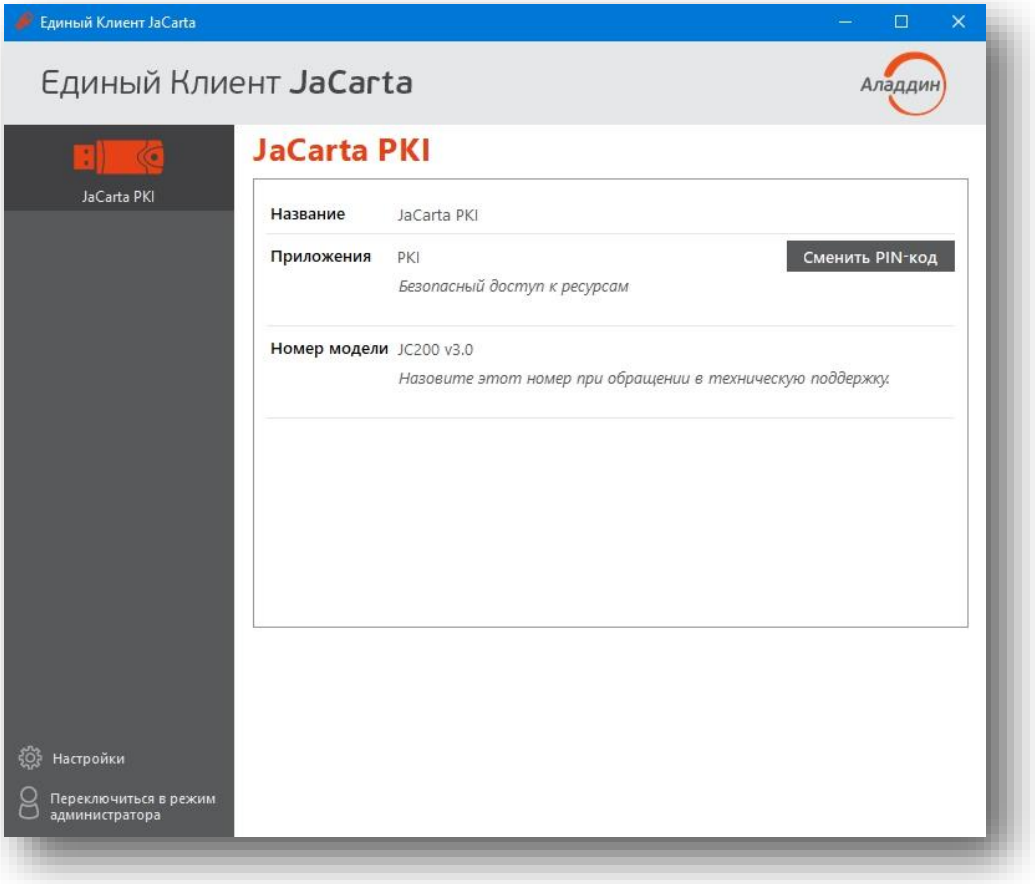

Рисунок 2 – Единый Клиент JaCarta

После нажатия кнопки <Сменить PIN-код> будет отображено окно (см. Рисунок 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> будет отображено окно, представленное ниже (см. Рисунок 4).

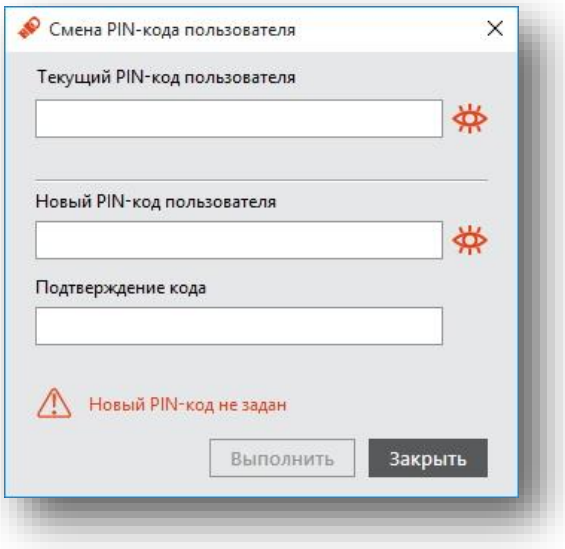

Рисунок 3 - Единый Клиент JaCarta. Смена PIN-кода пользователя

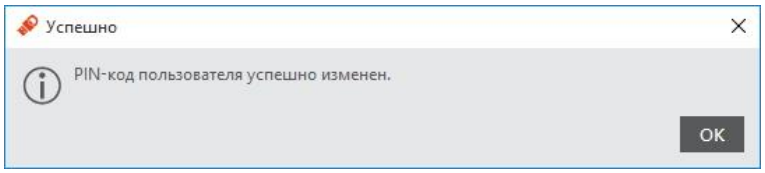

Рисунок 4 - Единый Клиент JaCarta. Информационное сообщение после успешной смены PIN-кода

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 администратора] – позволяет просматривать полные сведения о подсоединённых электронных ключах и предоставляет доступ ко всем операциям с электронными ключами.

Для переключения в режим администратора необходимо в окне Единый Клиент JaCarta нажать по элементу управления <Переключиться в режим администратора> (см. Рисунок 5).

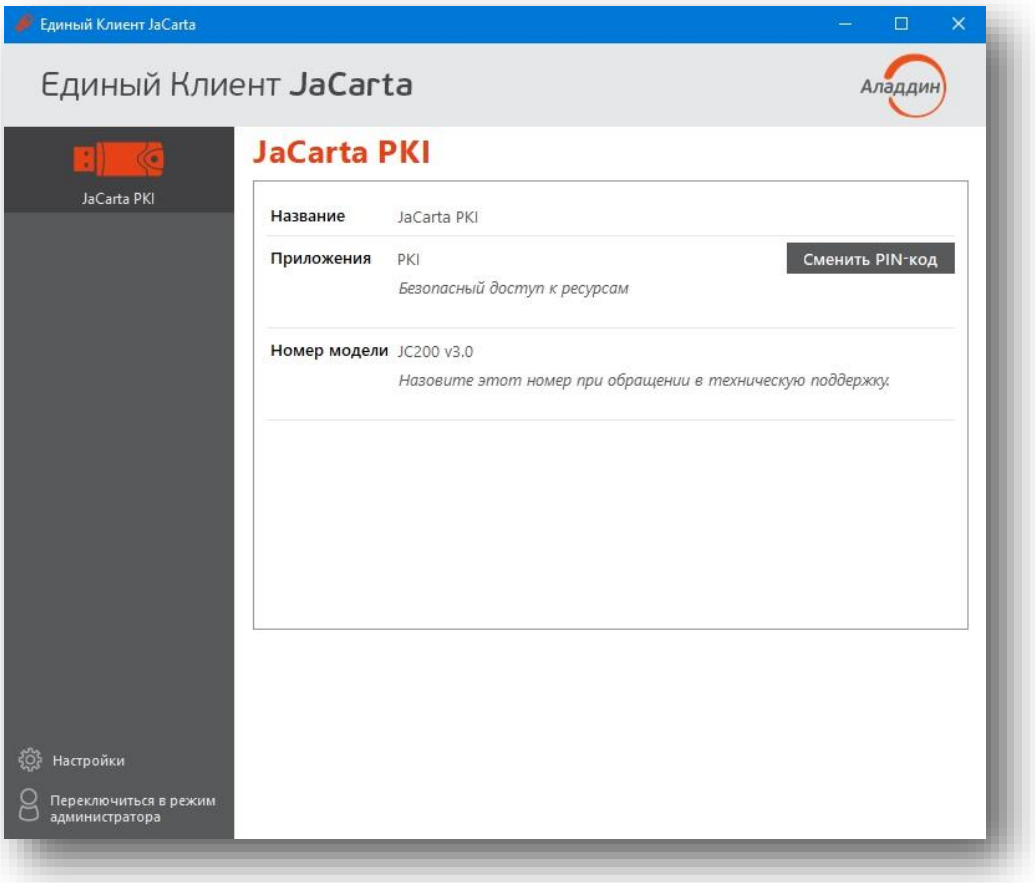

Рисунок 5 - Единый Клиент JaCarta. Главное окно. Переход в режим администратора

Для переключения в режим пользователя необходимо в главном окне Единый Клиент JaCarta нажать по элементу управления <Переключиться в режим пользователя> (см. Рисунок 6).

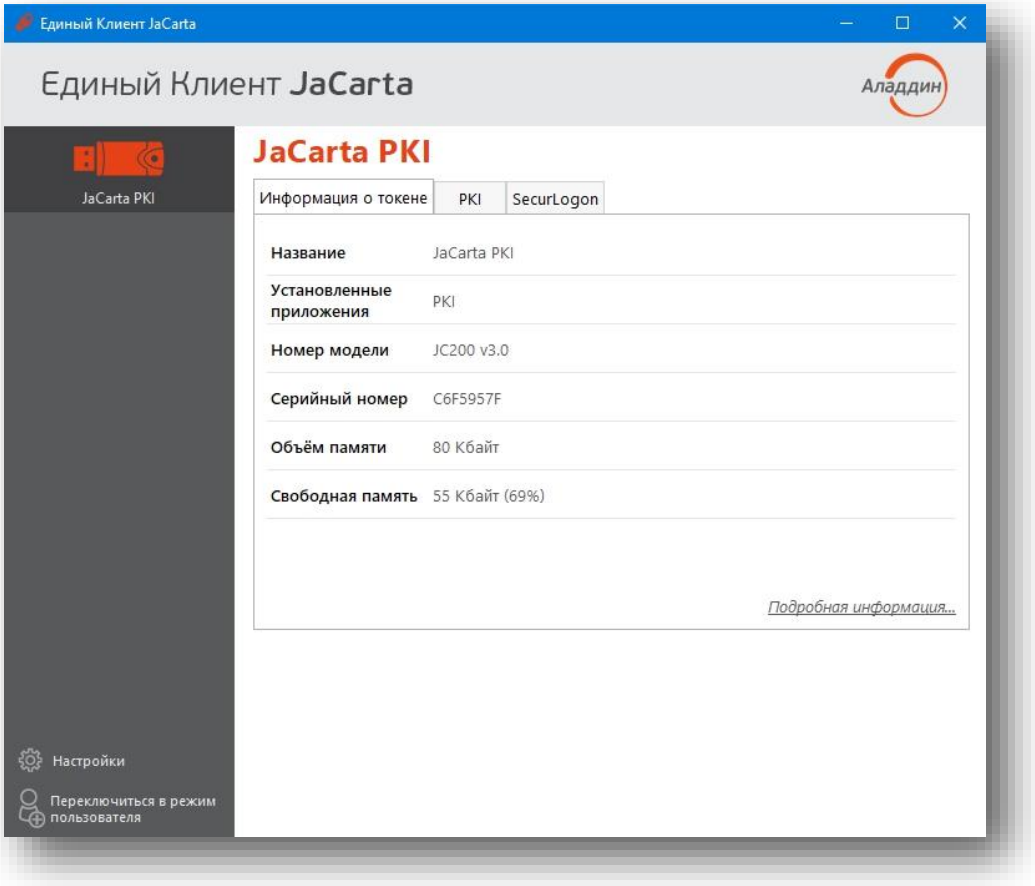

Рисунок 6 - Единый Клиент JaCarta. Главное окно. Переход в режим пользователя

3.4 Установка лицензии

Установить лицензию JaCarta SecurLogon можно двумя способами:

1. В режиме пользователя: через меню [Настройки] в окне Единый Клиент JaCarta;
2. В режиме администратора: через вкладку [SecurLogon] в окне Единый Клиент JaCarta.

Чтобы установить лицензию, необходимо обладать правами администратора.

В случае установки лицензии через вкладку [SecurLogon] в окне Единый Клиент JaCarta необходимо подсоединить электронный ключ к компьютеру.

В случае установки лицензии через меню [Настройки] в окне Единый Клиент 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 нажать кнопку <Настройки> в левом нижнем углу главного окна (см. Рисунок 7).

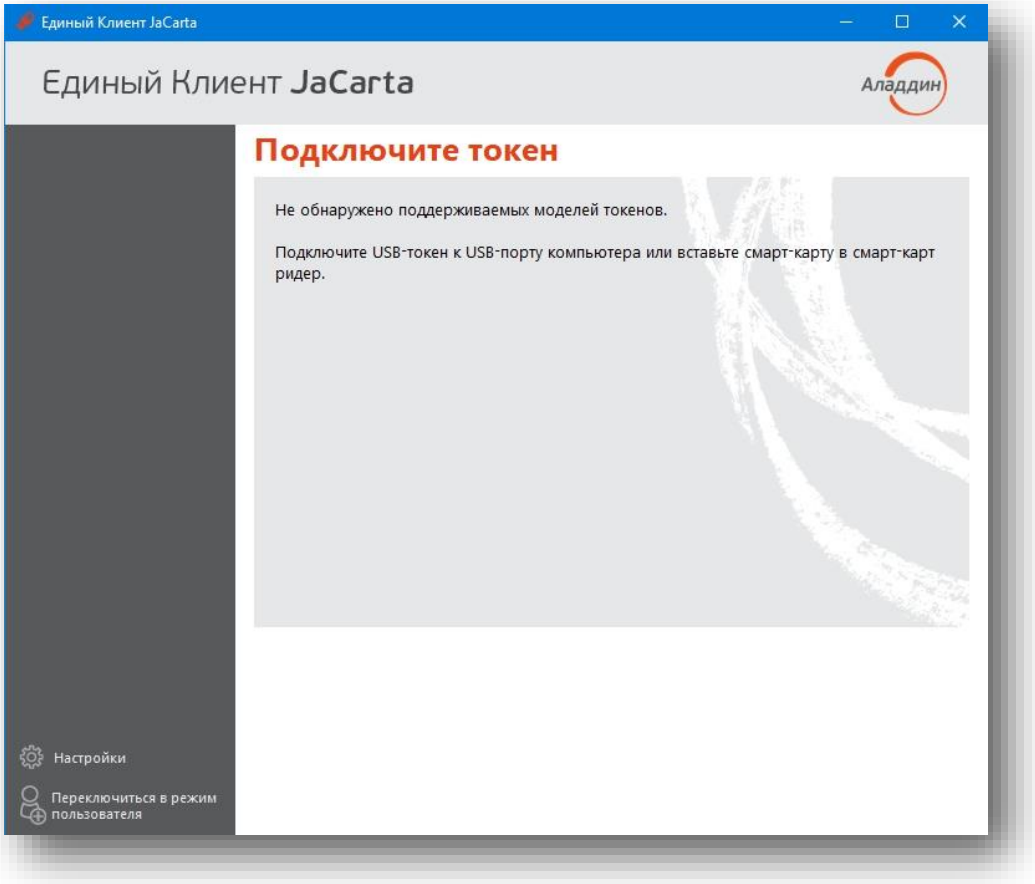

Рисунок 7 - Единый Клиент JaCarta. Главное окно. Элемент управления <Настройки>

2. В отобразившемся окне выбрать вкладку [SecurLogon] и нажать кнопку <Установить лицензию SecurLogon> (см. Рисунок 8).

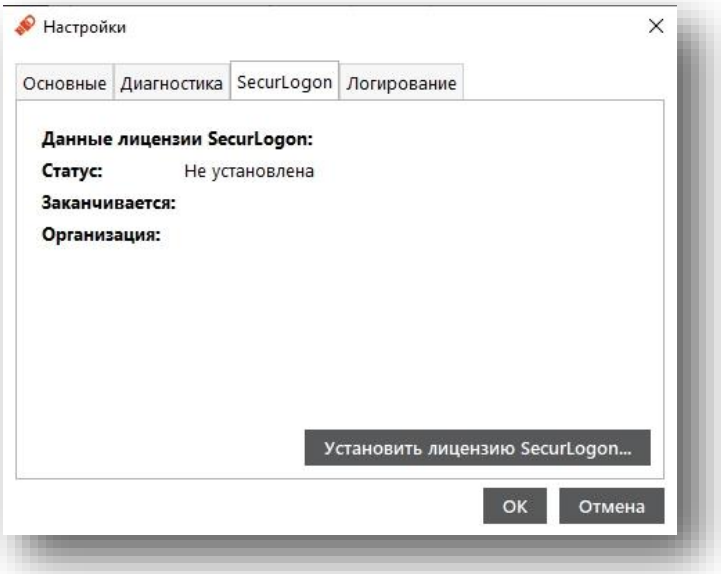

Рисунок 8 - Единый Клиент JaCarta. Окно [Настройки]. Вкладка [SecurLogon]

3. В отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку <Открыть>.

4. После установки лицензии в отобразившемся окне нажать кнопку <OK>.

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 переключиться в режим администратора, перейти на вкладку [SecurLogon] и в поле лицензии [Статус] нажать ссылку <установить> (см. Рисунок 9);

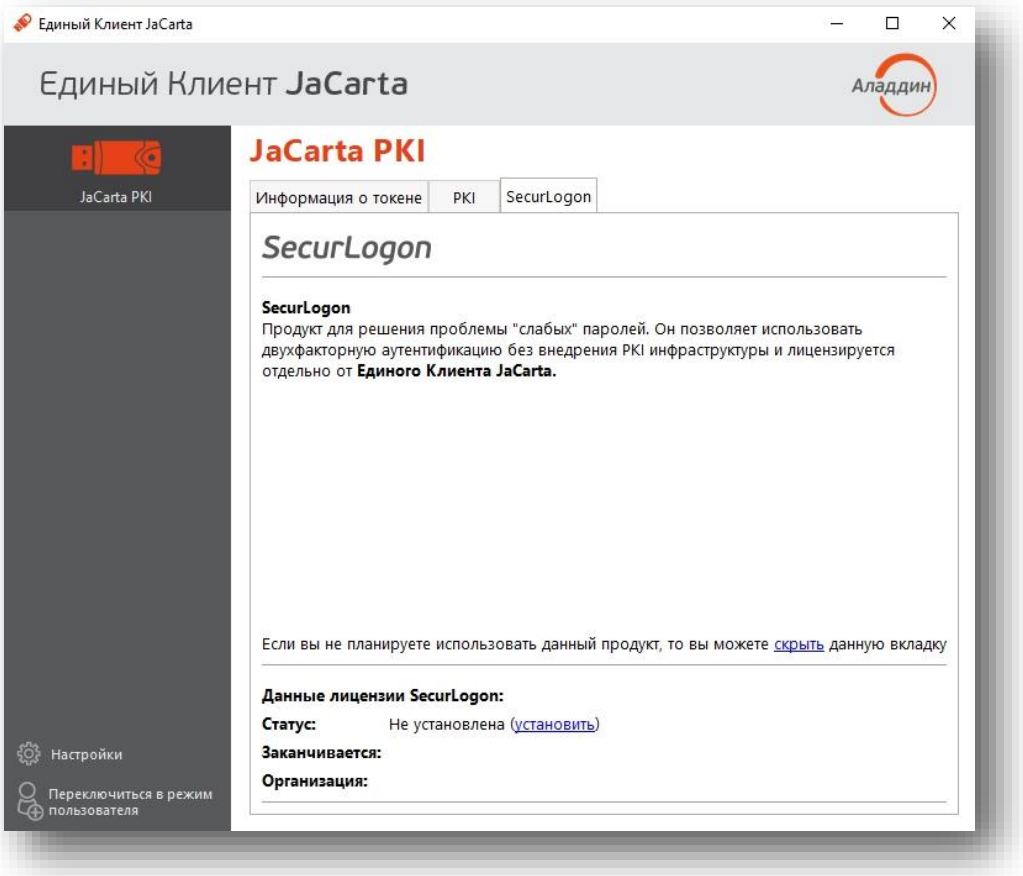

Рисунок 9 - Единый Клиент JaCarta. Вкладка [SecurLogon]

2. Далее в отобразившемся окне необходимо указать путь к файлу лицензии и нажать кнопку <Открыть>;
3. При успешном завершении операции вкладка [SecurLogon] примет вид, приведенный на Рисунок 10.

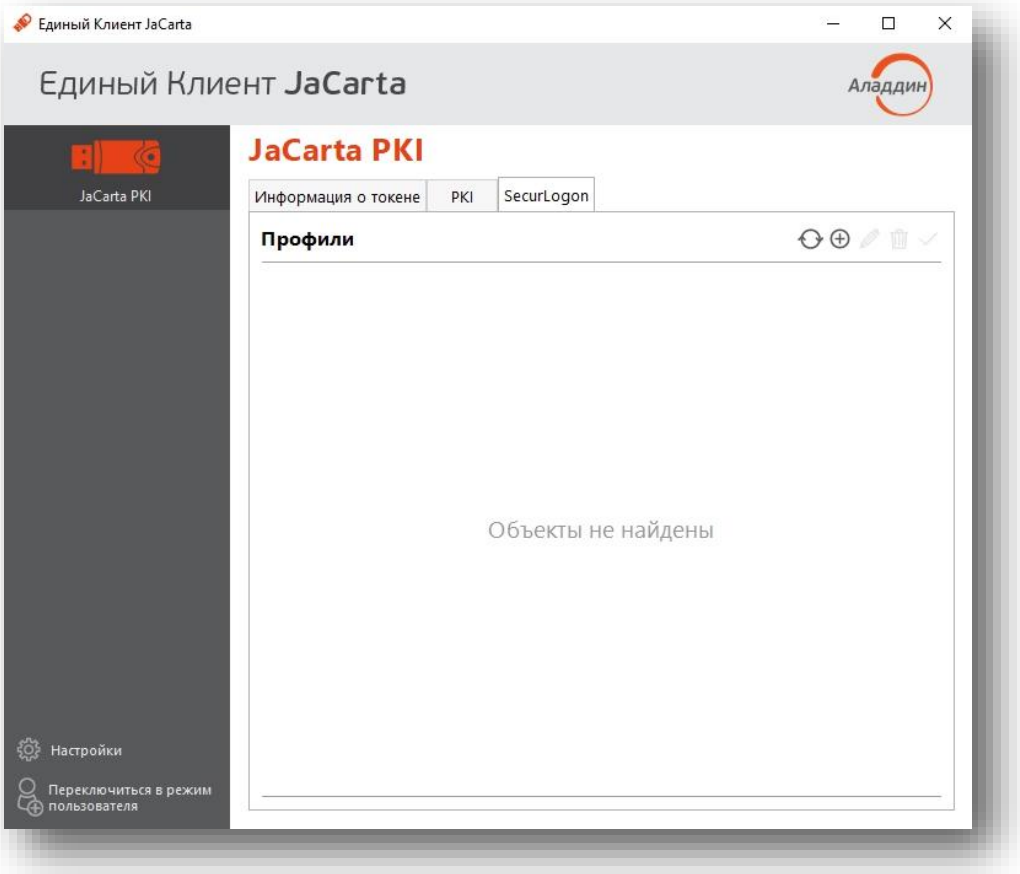

Рисунок 10 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Лицензия установлена успешно

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];

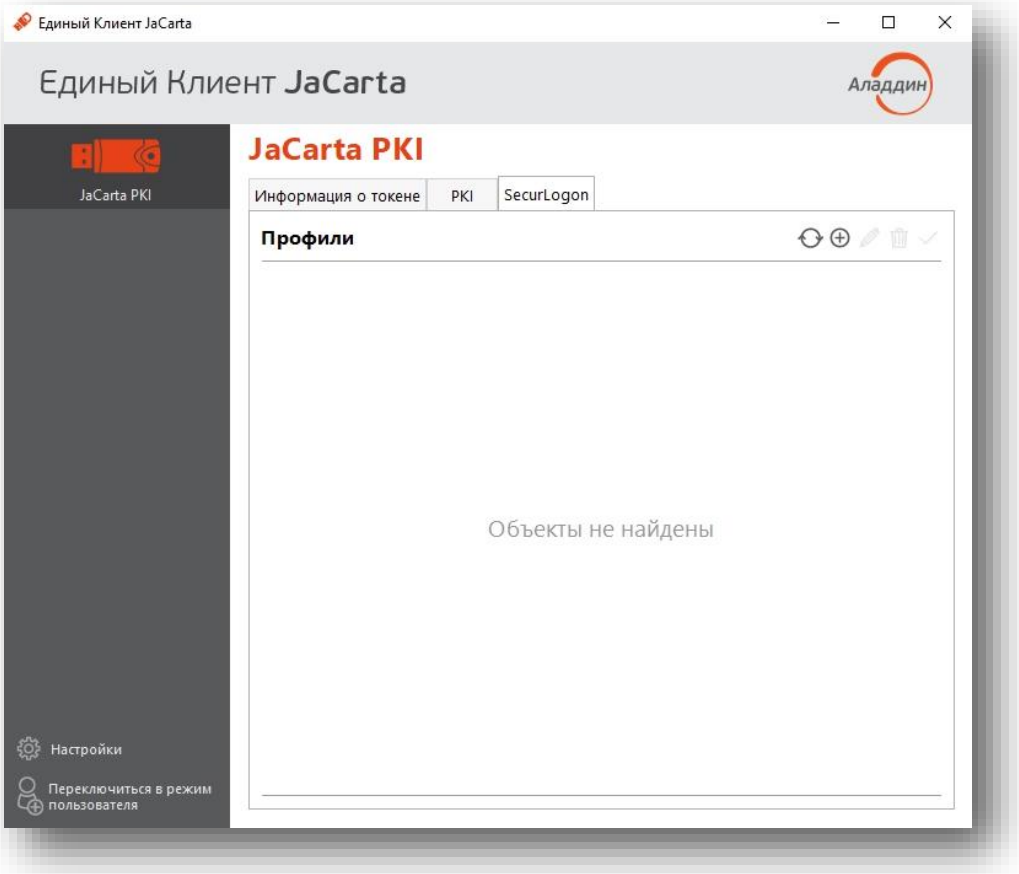

Рисунок 11 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Профили

3. Нажать на элемент ⊕ (см. Рисунок 11);

В зависимости от того, создаётся ли профиль JaCarta SecurLogon для локальной учётной записи или для учётной записи в домене ОС Microsoft Windows. Окно создания профиля может быть двух видов: для локальной учетной записи см. Рисунок 12, для учетной записи в домене ОС Microsoft Windows - см. Рисунок 13.

4. В окне [Создание профиля SecurLogon] (см. Рисунок 12 или Рисунок 13) следует заполнить поля, описание которых приведено в Таблица 1, и нажать кнопку <Создать>;

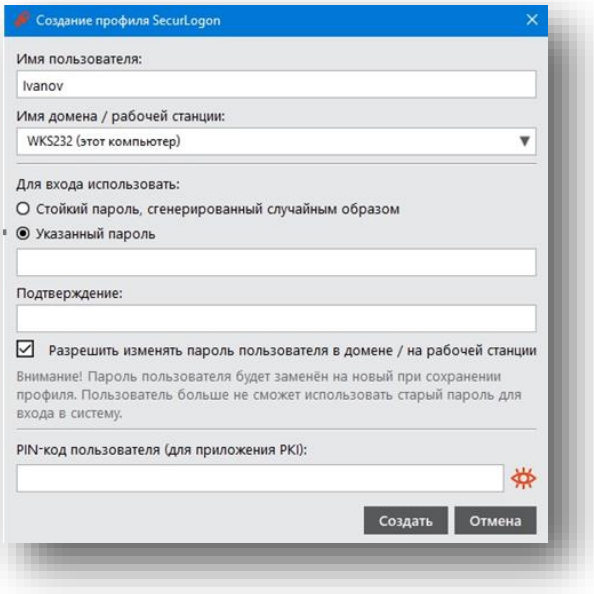

Рисунок 12 - [Создание профиля SecurLogon]. Окно создания локальной учетной записи

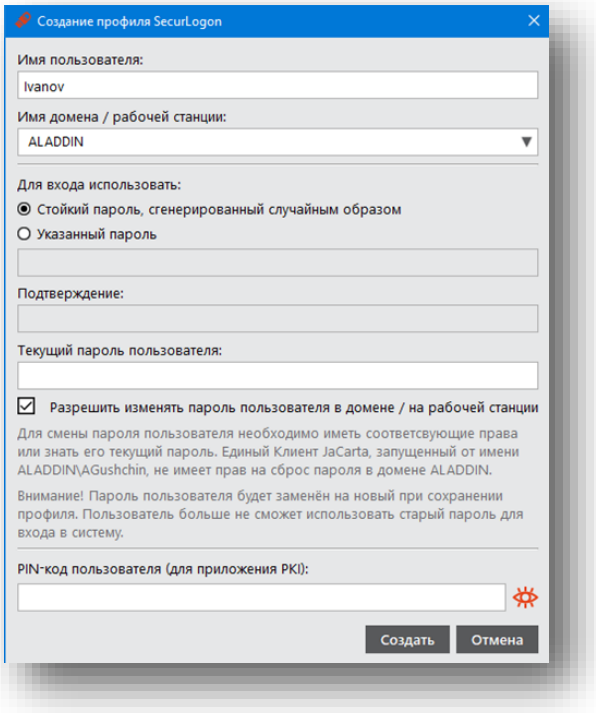

Рисунок 13 – [Создание профиля SecurLogon]. Окно создания учетной записи в домене ОС Microsoft Windows

Таблица 1 - Атрибуты профиля JaCarta SecurLogon

Название настройки	Описание настройки	
	Рабочая станция	Домен
[Имя пользователя]	Задает имя пользователя, для которого будет создан 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	
[Для входа использовать]	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)
[Имя пользователя для домена]	Не актуально 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)
[Пароль для домена]	Не актуально 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)
[Разрешить изменять пароль пользователя в домене / на рабочей станции]	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> (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
[PIN-код пользователя (для приложения PKI)]	В поле необходимо ввести текущий PIN-код электронного ключа

5. Созданный профиль будет отображен в окне Единый Клиента JaCarta на вкладке [SecurLogon]. На Рисунок 14 приведен вид локальной учетной записи, на Рисунок 15 - учетной записи в домене ОС Microsoft Windows.

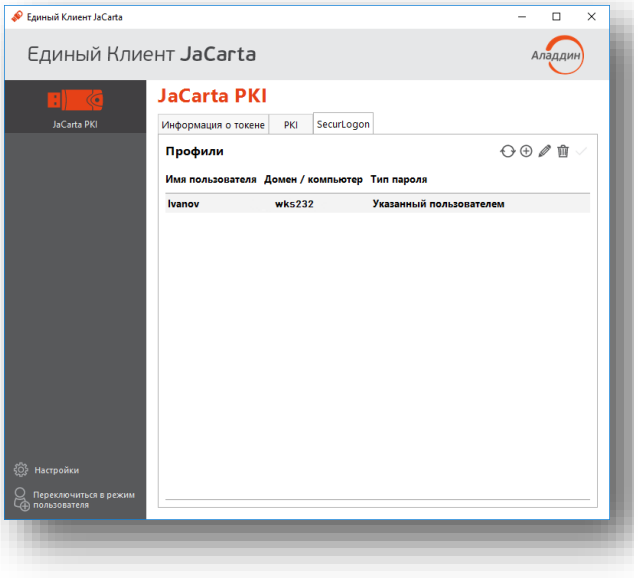

Рисунок 14 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Профиль локальной учетной записи

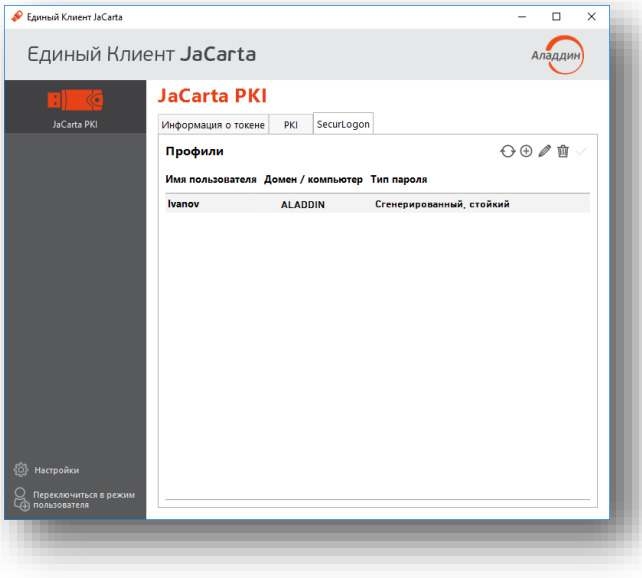

Рисунок 15 – Единый Клиент JaCarta. Вкладка [SecurLogon]. Профиль учетной записи в домене ОС Microsoft Windows

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 – такой профиль будет отображаться первым при входе в систему.

Для установки профиля 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 главном окне нажать на элементе ✓ (см. Рисунок 16) или правой кнопкой мыши у выбранного профиля вызвать контекстное меню и выбрать пункт <Установить по умолчанию>;

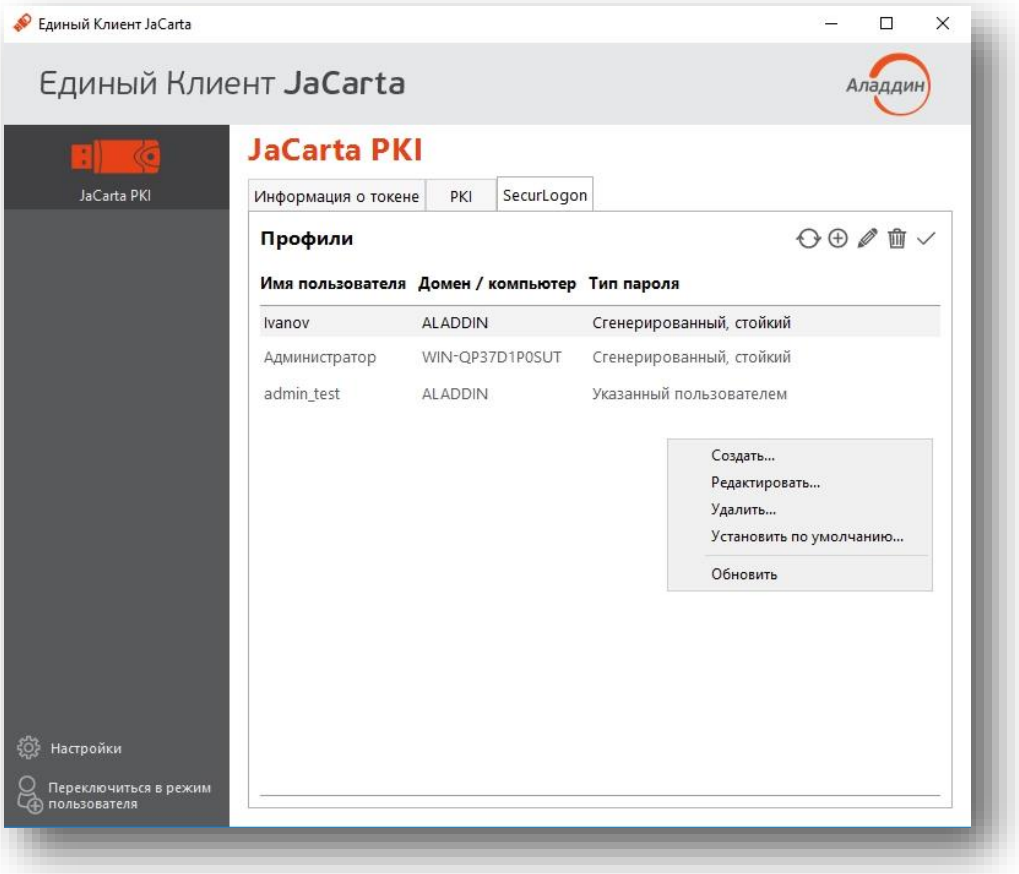

Рисунок 16 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Установка профиля по умолчанию

5. Далее в отобразившемся окне (см. Рисунок 17) ввести PIN-код в соответствующем поле и нажать <OK>;

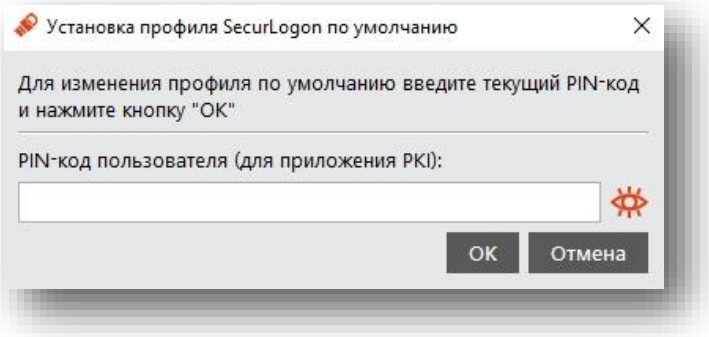

Рисунок 17 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Окно [Установка профиля SecurLogon по умолчанию]

6. Выбранный ранее профиль в окне Единый Клиент JaCarta должен стать профилем по умолчанию, он будет выделен жирным шрифтом среди других профилей (см. Рисунок 18).

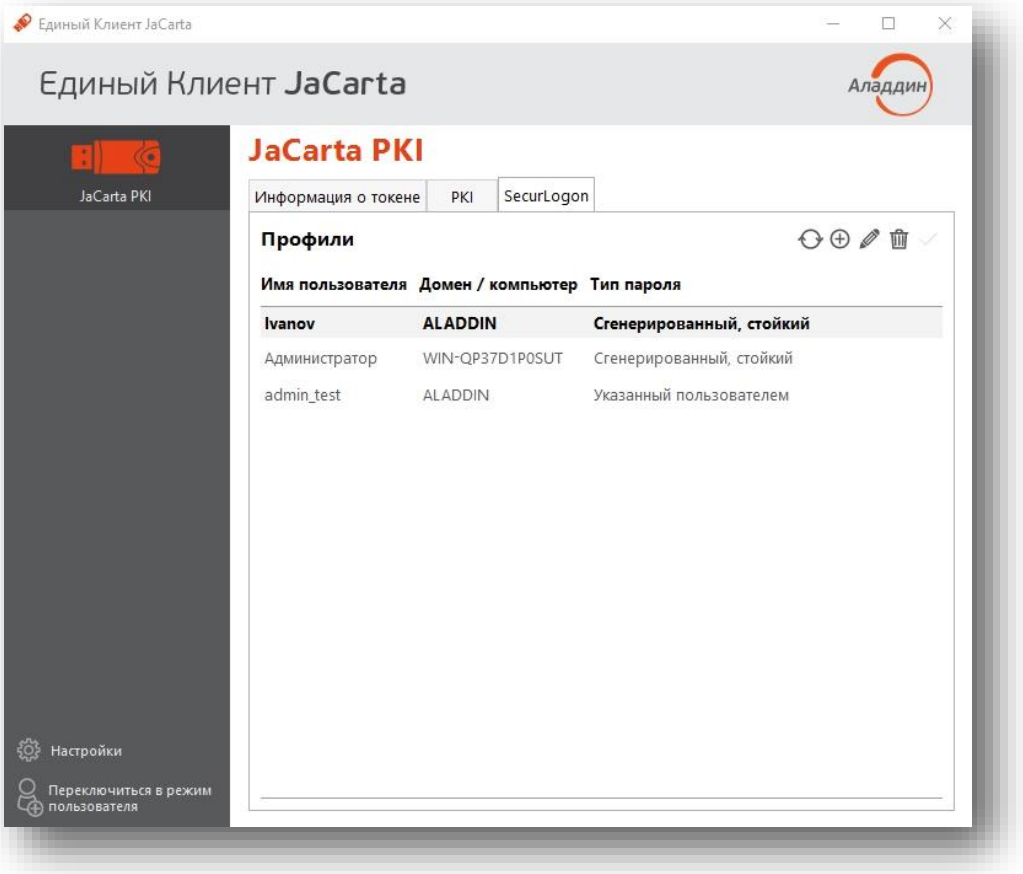

Рисунок 18 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Установленный профиль по умолчанию

4.1.3 Редактирование существующего профиля

Для редактирования профиля 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. Выбрать профиль, который необходимо изменить;
4. Нажать на элемент  (см. Рисунок 19) или с помощью правой кнопки мыши на выбранном профиле вызвать контекстного меню и выбрать пункт <Редактировать>;

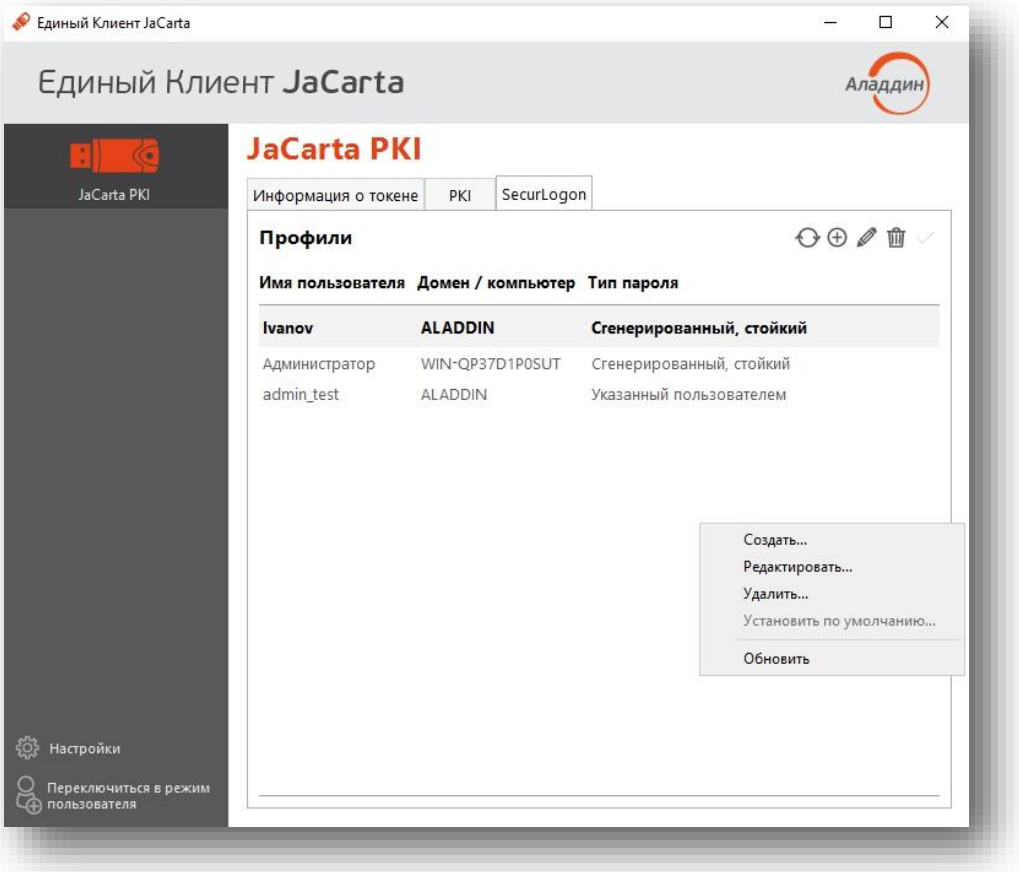

Рисунок 19 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Редактирование профиля

5. В отобразившемся окне (см. Рисунок 20) выполнить необходимые изменения и нажать <Сохранить>.

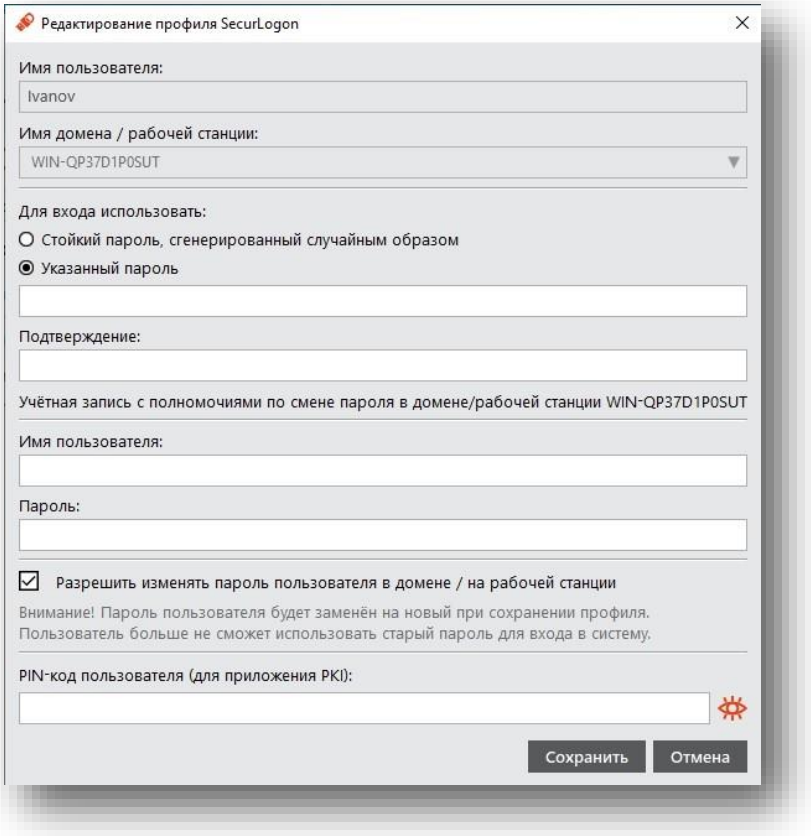

Рисунок 20 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Окно [Редактирование профиля SecurLogon]

4.1.4 Удаление профиля

Для удаления профиля 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 элемент или у выбранного профиля вызвать контекстное меню и выбрать пункт <Удалить> (см. Рисунок 21).

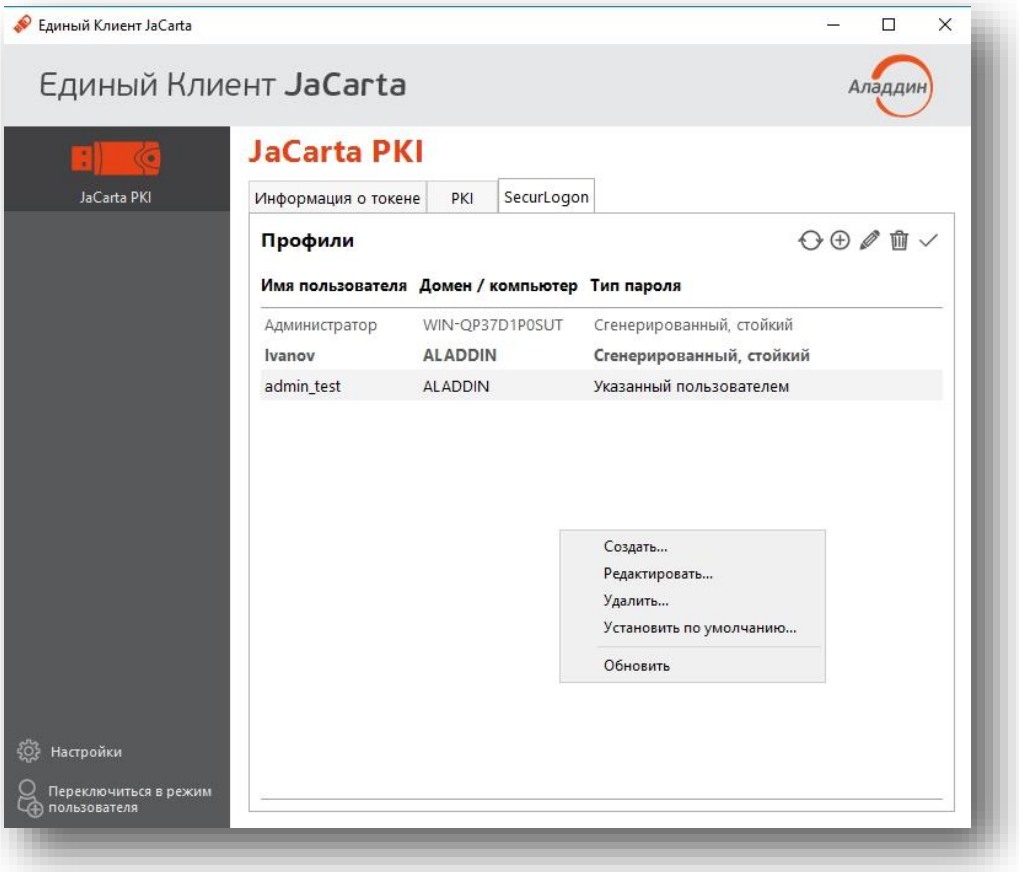

Рисунок 21 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Удаление профиля

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. Рисунок 22).

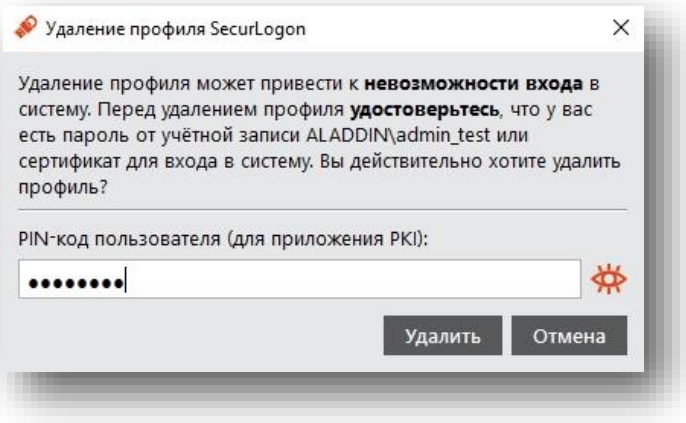

Рисунок 22 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Ввод PIN-кода для удаления профиля

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. Рисунок 23).

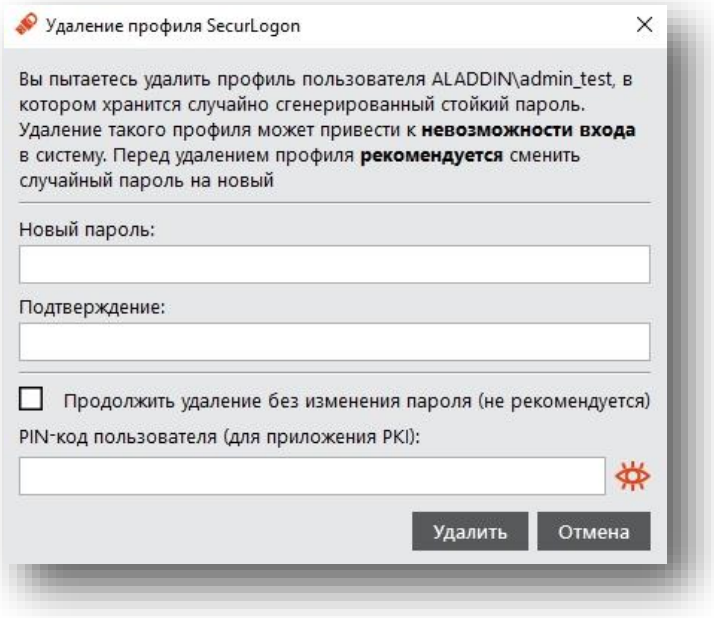

Рисунок 23 - Единый Клиент JaCarta. Вкладка [SecurLogon]. Окно [Удаление профиля SecurLogon] при удалении профиля со «стойким паролем»

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 будет сохранен случайный пароль, сгенерированный при создании профиля JaCarta SecurLogon.

> *Внимание! Не рекомендуется устанавливать этот флажок, так как 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 на компьютере, на которым установлены средства управлениям контроллером домена.

Для запуска административного шаблона JaCarta SecurLogon и отображения его настроек необходимо выполнить следующие действия:

1. Нажать на клавиатуре сочетание клавиш `Win+R`, в появившемся окне набрать `gpmc.msc` и нажать <OK> (см. Рисунок 24);

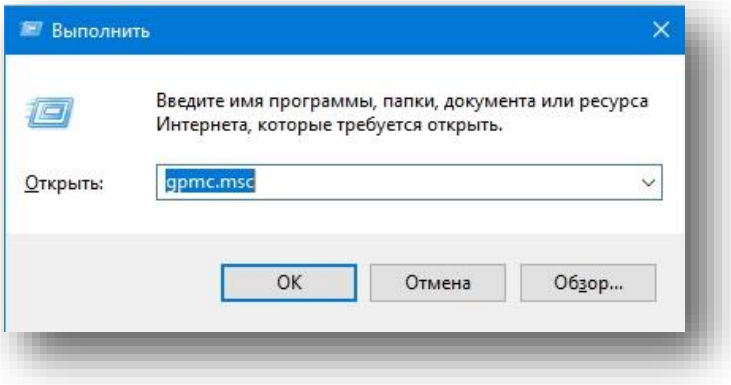

Рисунок 24 – Вызов окна командной строки

2. В появившемся окне (см. Рисунок 25) следует последовательно выбрать [Лес], [Домены], [имя_домена], далее нажать правой кнопкой мыши на пункте <Default Domain Policy> (Политика домена по умолчанию) и из контекстного меню выбрать опцию <Изменить>;

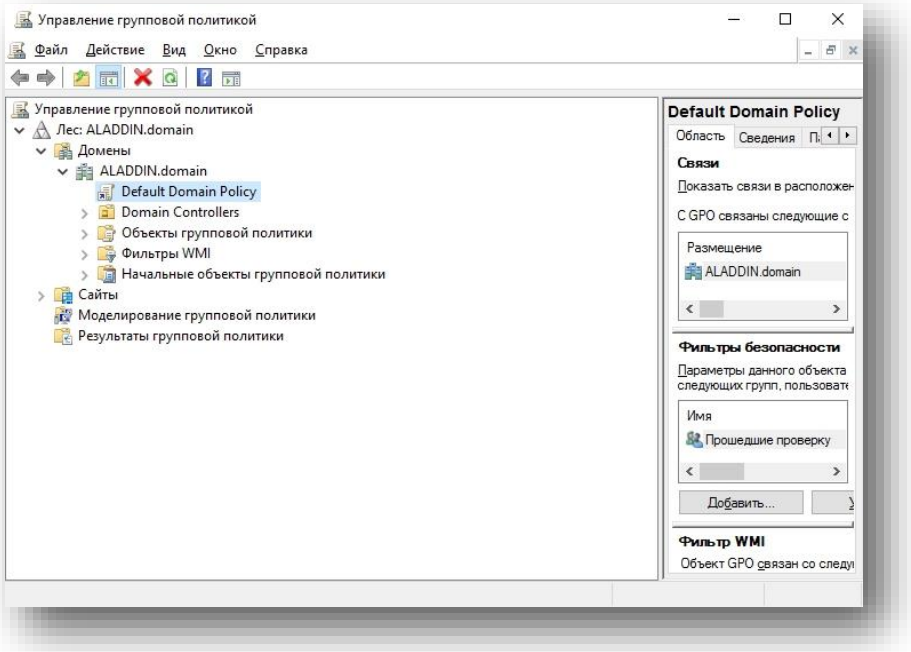

Рисунок 25 – Окно [Управление групповой политикой]

3. В появившемся окне (см. Рисунок 26) следует последовательно выбрать [Конфигурация компьютера], [Политики], [Административные шаблоны], [JaCarta SecurLogon];

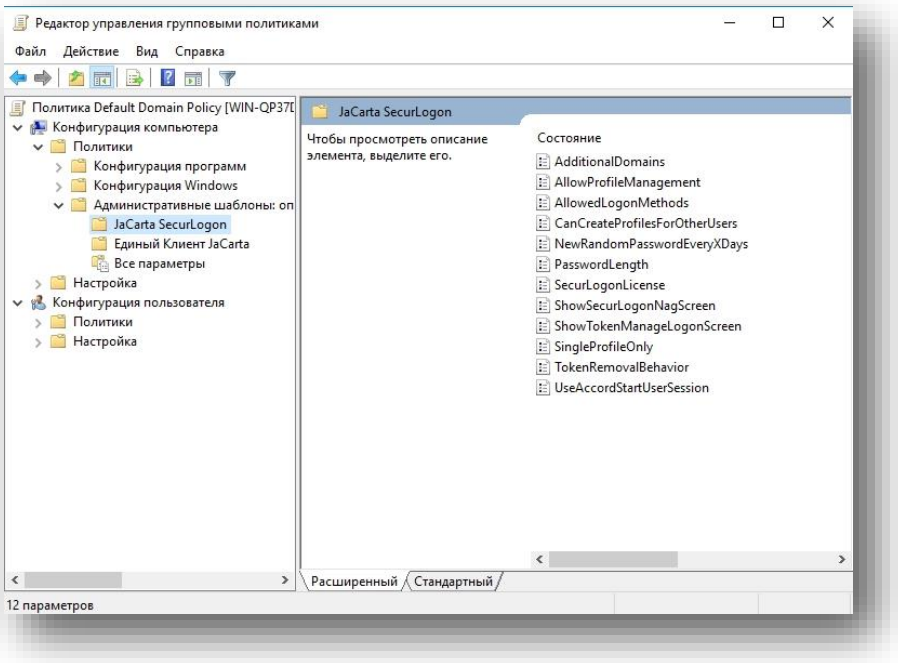

Рисунок 26 - Окно [Редактор управления групповыми политиками]

4. Редактирование административного шаблона JaCarta SecurLogon происходит 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

Для запуск административного шаблона JaCarta SecurLogon и отображения его настроек необходимо выполнить следующие действия:

1. Нажать на клавиатуре сочетание клавиш `Win+R`, в появившемся окне набрать `gpedit.msc` и нажать <OK> (см. Рисунок 27);

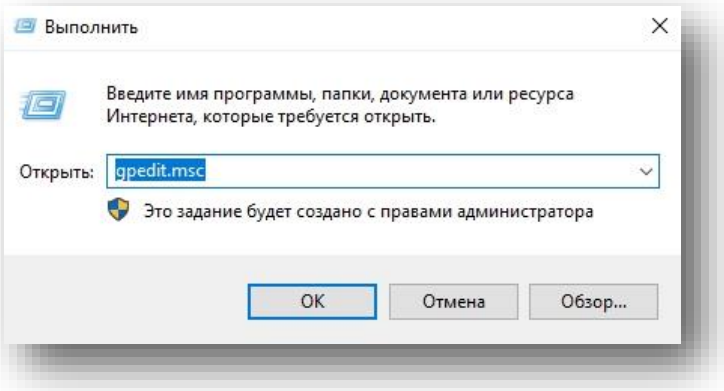

Рисунок 27 - Вызов окна командной строки

2. В появившемся окне последовательно выбрать [Конфигурация компьютера], [Административные шаблоны], [Компоненты Windows], [JaCarta SecurLogon] (см. Рисунок 28);

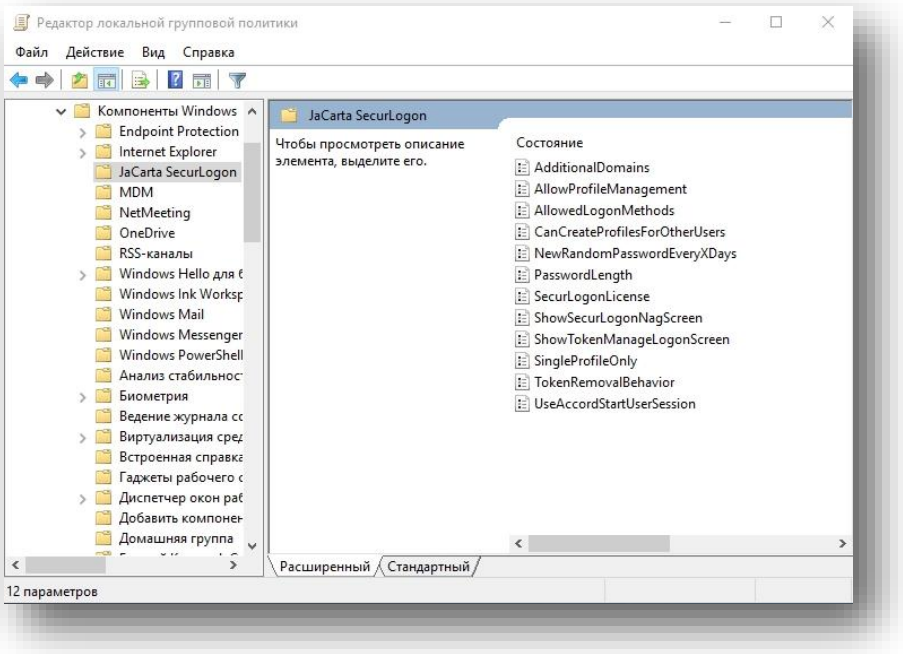

Рисунок 28 – Окно [Редактор локальной групповой политики]

3. Редактирование административного шаблона JaCarta SecurLogon происходит 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.

4.3 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, описанные в документе [Единый Клиент JaCarta. Руководство администратора для Windows].

5. Приложение А

Таблица 2 – Настройки административного шаблона

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 использовано 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 использовано значение по умолчанию (последний столбец настоящей таблицы); <Отключено> – будут использованы 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;	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

		<ManualPasswordLogon> – пароль для профиля SecurLogon вводится вручную; <RandomPasswordLogon> – для профиля SecurLogon генерируется случайный пароль		
CanCreateProfilesForOtherUsers (Создание профилей для других пользователей)	Разрешает или запрещает пользователю создавать профили для других пользователей	<Не задано> – будет использовано 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 использовано значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); <Включено> – станет доступным для редактирования 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 использовано значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); <Включено> – станет доступным для редактирования соответствующее поле, в котором нужно задать 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 использовано значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); <Включено> – станет доступным для редактирования соответствующее поле, в которое необходимо полностью скопировать содержимое файла лицензии (для этого файл лицензии можно открыть в текстовом редакторе);	Пустая строка	Пустая строка

		<Отключено> – лицензия не устанавливается (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
ShowTokenManageLogonScreen	Определяет отображать или не отображать плитку [Управление токеном] на logon screen Windows	<Не задано> – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); <Включено> – плитка [Управление токеном] отображается; <Отключено> – плитка [Управление токеном] не отображается	Включено	Включено
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	Не выполнять никаких действий	Не выполнять никаких действий

		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		
UseAccordStartUserSession	Определяет использовать или не использовать ПАК СЗИ НСД АККОРД при входе пользователя в операционную систему	<Включено> - будет использован ПАК СЗИ НСД АККОРД при входе пользователя в операционную систему по профилю JaCarta SecurLogon; <Отключено> или <Не задано> - не будет использован ПАК СЗИ НСД АККОРД при входе пользователя в операционную систему по профилю JaCarta SecurLogon	Отключено	Отключено
SetSecurLogonAsDefaultLogonProvider (Установка JaCarta SecurLogon провайдером по умолчанию)	Разрешает или запрещает использовать JaCarta SecurLogon как Logon Provider по умолчанию	<Не задано> – будет использоваться значение по умолчанию, заданное в шаблоне (последний столбец настоящей таблицы); <Включено> – разрешает использовать JaCarta SecurLogon как Logon Provider по умолчанию; <Отключено> – запрещает использовать JaCarta SecurLogon как Logon Provider по умолчанию	Включено	Включено

Таблица 3 – Значение PIN-кодов по умолчанию

Параметры	**eToken PRO Anywhere** **eToken NG-OTP (Java)** **JaCarta PRO**	**JaCarta PKI** **JaCarta PKI/Flash** **JaCarta PKI/BIO**	**JaCarta-2 PKI/ГОСТ** **JaCarta-2 PRO/ГОСТ**	**JaCarta LT**
Приложение	PKI	PKI и PKI/BIO	ГОСТ	STORAGE
PIN-код пользователя по умолчанию	1234567890	11111111	Не установлен	1234567890
PIN-код администратора по умолчанию	1234567890	00000000		Нет[4]

[4] При необходимости пользователь может задать PIN-администратора при форматировании электронного ключа. В дальнейшем этот PIN-администратора будет требоваться для повторного форматирования

6. Контакты

6.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, 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.ru (общий)

Web: https://www.aladdin.ru

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

6.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin.ru/support/.

7. Ресурсы

7.1 Сокращения и аббревиатуры

ГОСТ	Государственный стандарт
ОС	Операционная система
ПО	Программное обеспечение
ПК	Персональный компьютер
PIN	Конфиденциальная аутентификационная информация
PKI	Инфраструктура открытых ключей
USB	(Universal Serial Bus) универсальная последовательная шина

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