GIS ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности

Часть 5. Управление токенами

Санкт-Петербург, 2024

Аннотация

В документе содержатся сведения о подсистеме управления жизненным циклом токенов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4»:

– назначение подсистемы и ее основные функциональные возможности;

– описание интерфейса подсистемы и основные принципы работы с ним.

Содержание

Введение 5
1 Назначение подсистемы управления жизненным циклом токенов 6
2 Общий порядок работы при назначении токена пользователю 7
3 Управление токенами в иерархии серверов 9
4 Управление токенами 12
4.1 Добавление токена в подсистему 12
4.2 Инициализация токена 15
4.3 Профили инициализации 17
4.4 Поиск токена 23
4.5 Удаление токена 24
4.6 Просмотр сертификатов на токене 25
4.7 Смена PIN-кода токена 28
4.8 Разблокировка токена 32
4.9 Инвентарный номер/Комментарий 35
4.10 Выпуск токена 36
4.11 История актов 37
5 Управление пользователями 40
5.1 Поиск пользователя 40
5.2 Карточка пользователя 41
5.3 Назначение токена пользователю 42
5.4 Привязка пользователя SafeNode 60
5.5 Удаленное назначение токена пользователю 63
6 Сертификаты на устройстве 70
6.1 Состояния сертификата 71
6.2 Жизненный цикл токена с выпуском управляемого сертификата 72
6.3 Жизненный цикл токена без выпуска управляемого сертификата 79
7 Синхронизация 81
7.1 Синхронизация сертификатов для входа, выпущенных подсистемой 85

7.2 Синхронизация наблюдаемых сертификатов, используемых для входа, выпущенных сторонними средствами 87
7.3 Синхронизация наблюдаемых сертификатов, не используемых для входа 87
7.4 Синхронизация токенов, не содержащих сертификаты 88
8 Общие настройки 89
8.1 Настройка дополнительных параметров 90
8.2 Настройка почтовых уведомлений 91
8.3 Шаблоны актов 96
Приложение 1. Описание возможных алгоритмов синхронизации токенов 101
Перечень сокращений 118

Введение

Подсистема управления жизненным циклом токенов предназначена для управления носителями пользователей на протяжении всего жизненного цикла.

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

Важная информация
Указания, требующие особого внимания.

Дополнительная информация
Указания, позволяющие упростить работу с подсистемой.

1 Назначение подсистемы управления жизненным циклом токенов

Подсистема предназначена для управления устройствами аутентификации пользователей на протяжении всего жизненного цикла.

Подсистема обеспечивает:

– учет токенов в системе;

– управление токенами (назначение пользователям, приостановка использования, вывод из использования);

– аудит в течении всего жизненного цикла.

Основные задачи, решаемые подсистемой:

– регистрация токенов в системе;

– назначение токенов пользователям;

– приостановка/возобновление использования токенов;

– вывод токенов из использования (отзыв цифровых сертификатов на устройствах);

– запись цифровых сертификатов на токен;

– удаление токенов из системы;

– уведомление пользователей и администратора о состоянии цифровых сертификатов на токенах (действителен, отозван, истекает, отклонен, одобрен и т.д.);

– поиск и фильтрация информации о токенах и пользователях в базе данных подсистемы;

– формирование актов и отслеживание истории актов по результатам операций выдачи токена пользователю, изъятия токена и удаления токена из системы.

2 Общий порядок работы при назначении токена пользователю

Общий порядок работы в подсистеме жизненного цикла токена при назначении токена пользователю следующий:

1) Токен регистрируется в подсистеме жизненного цикла токена (раздел **Добавление токена в подсистему**).

Регистрация токена в подсистеме возможна с использованием инициализации и без нее (раздел ***«Инициализация токена»***):

– в случае использования инициализации все данные, хранимые на токене, удаляются, и задаются новые значения PIN-кодов пользователя и администратора, и ограничения на них;

– если инициализация не используется, все данные (например, сертификаты, имеющие на токене) остаются на токене, PIN-коды пользователя и администратора не меняются.

При инициализации возможно не вводить для каждого токена новые значения PIN-кодов и ограничения для них, а использовать предварительно заведенный для нужного типа устройства профиль инициализации (раздел ***«Профили инициализации»***).

2) Токен назначается пользователю (раздел ***«Назначение токена пользователю»***). При этом возможно выпустить пользователю токен, используемый для:

– учета,

– безопасного входа по паролю,

– входа по управляемому сертификату;

– входа по стороннему сертификату.

3) Дальнейшие действия с токеном, зависят от того, как был выпущен токен.

Токен, выпущенный для входа по управляемому сертификату (раздел ***«Жизненный цикл токена с выпуском управляемого сертификата»***), возможно:

– приостановить/возобновить использование (отключение токена на определенный промежуток времени, например, на время отпуска пользователя),

– вывести токен из использования (все сертификаты, записанные на токен, отзываются без возможности восстановления, например, в случае утери или в случае

его неисправности);

– изъять токен (привязка токена к пользователю удаляется, токен возвращается в эксплуатацию для последующего назначения).

Токен, выпущенный учета, безопасного входа по паролю и входа по стороннему сертификату (раздел ***«Жизненный цикл токена без выпуска управляемого сертификата»***), возможно только изъять.

3 Управление токенами в иерархии серверов

Иерархия управления серверов или иерархия масштабирования предполагает, что в сеть входит несколько серверов, между которыми делится нагрузка. При этом администратор безопасности может управлять всеми, входящими в иерархию, подчиненными серверами с консоли управления мастер-сервера (рисунок 3.1).

В том числе осуществлять управление токенами клиентских рабочих станций подчиненных серверов.

Пример 1

На рисунке 3.1 токен подключен к рабочей станции host6, являющейся клиентом подчиненного сервера Server2. Администратор безопасности хочет выдать токен, подключенный к host6, пользователю для входа по сертификату. При этом консоль управления и мастер-сервер находятся на мастер-сервере Server1.

По выданному токену, подключенному к host6, можно будет осуществить вход на всех клиентских рабочих станциях мастер-сервера Server1 и подчиненного сервера Server2.

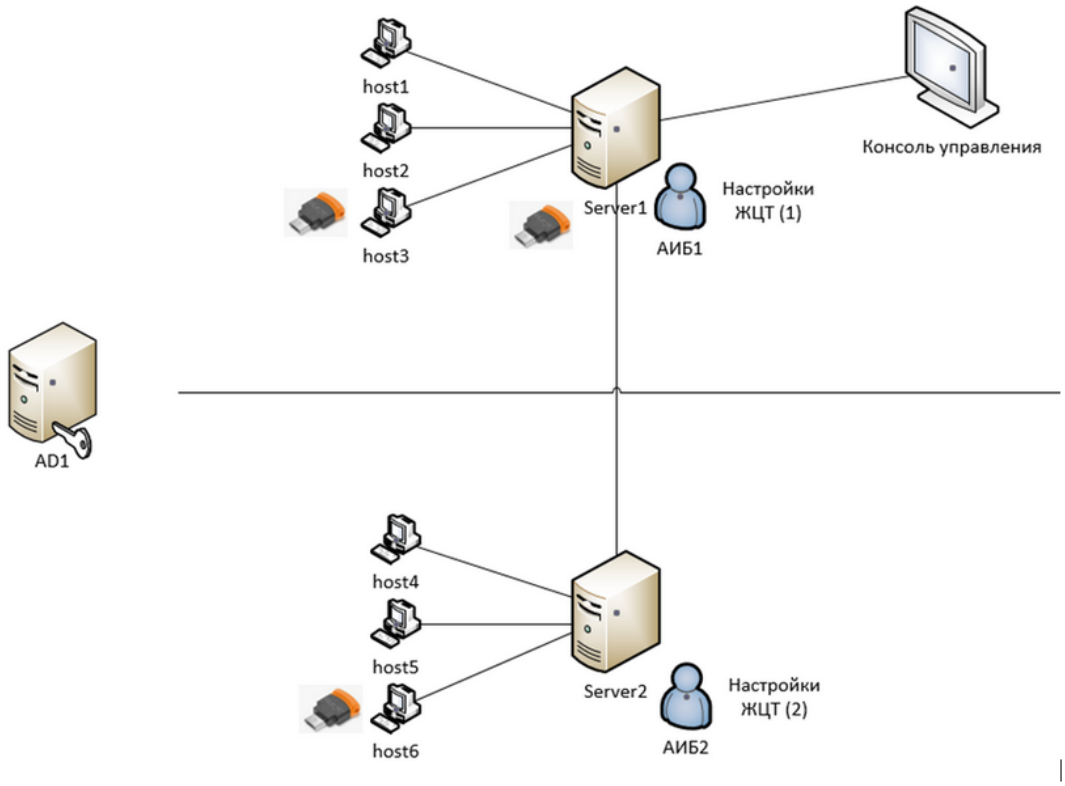


Рисунок 3.1 – Управление токенами в иерархии серверов

Пример 2

На рисунке 3.2 токен подключен к рабочей станции host6, являющейся клиентом

подчиненного сервера Server2. Администратор безопасности хочет выдать токен, подключенный к host6, пользователю для входа по сертификату. При этом консоль управления и мастер-сервер находятся на мастер-сервере Server1, мастер-сервер Server1 и его клиентские рабочие станции введены в домен AD1, а подчиненный сервер Server2 и его клиентские рабочие станции введены в домен AD2.

По выданному токену, подключенному к host6, можно будет осуществить вход на всех клиентских рабочих станциях подчиненного сервера Server2. На клиентских рабочих станциях мастер-сервера Server1 вход будет невозможен, по причине вхождения в другой домен.

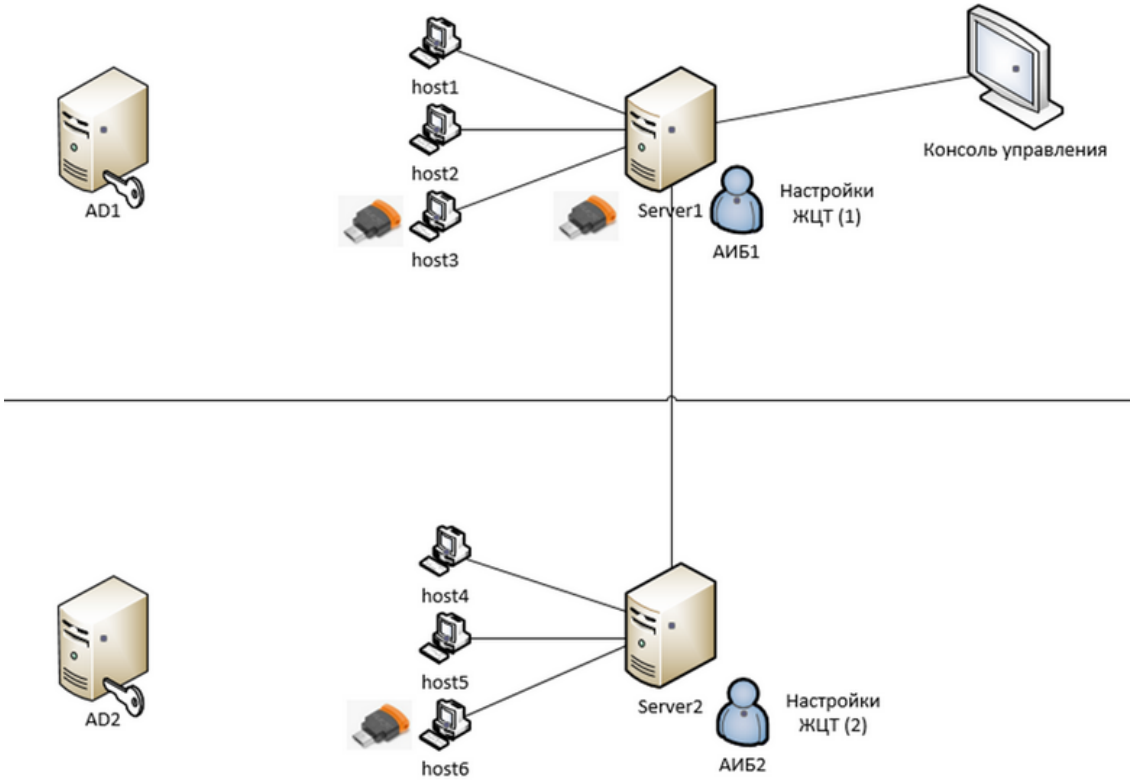


Рисунок 3.2 – Управление токенами в разных AD

При построении иерархии серверов список токенов с мастер-сервера передается по иерархии на все подчиненные серверы. При этом все управляемые токены, выпущенные мастер-сервером недоступны для редактирования на подчиненных серверах. Для токенов, выпущенных мастер-сервером, на подчиненных серверах доступна только операция просмотра содержимого токена (рисунок 3.3).

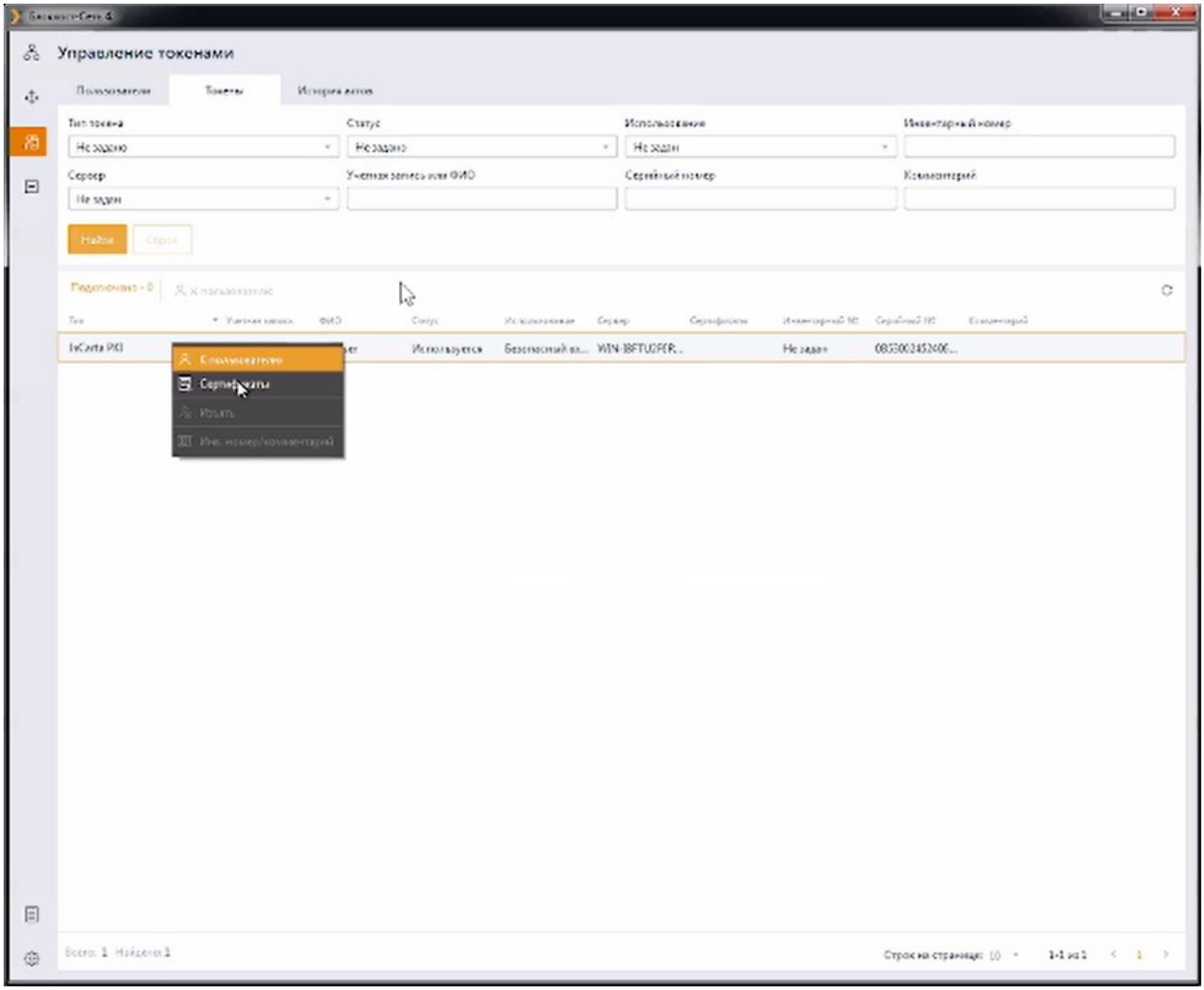


Рисунок 3.3 – Отображение токена с мастер-сервера

Если один и тот же токен выдан разным пользователям на мастер-сервере и подчиненном сервере, приоритет отдается токену, выпущенному мастер-сервером.

При этом запись о выдаче токена подчиненным сервером физически не затирается, а перекрывается записью с мастер-сервера. И при разрыве иерархии, когда список с мастер-сервера больше не будет приходить на подчиненный сервер, выдача с подчиненного сервера станет актуальной.

4 Управление токенами

Основная работа с подсистемой жизненного цикла токенов осуществляется во вкладках ***Пользователи, Токены*** и ***История актов***, доступные по кнопке .

Вкладка ***Токены*** предназначена для управления устройствами аутентификации (рисунок 4.1). Позволяет выполнять поиск токенов, просматривать сертификаты на них, изменять инвентарные номера токенов в списке, при необходимости добавлять комментарии, а также назначать токены пользователю.

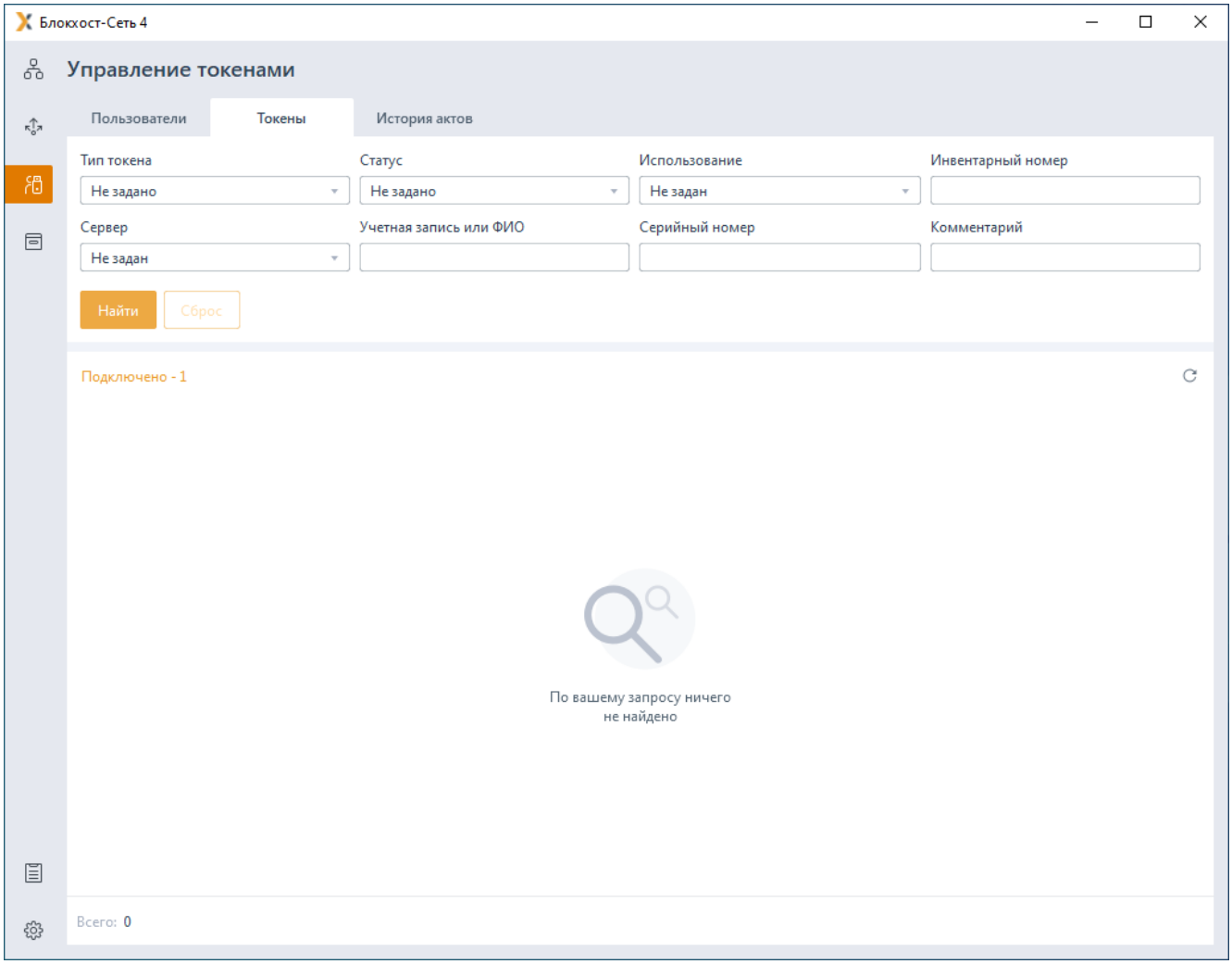


Рисунок 4.1 – Вкладка ***Токены***

4.1 Добавление токена в подсистему

Подключите токен к АРМ администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4».

Перейдите по ссылке ***Подключено*** (рисунок 4.2).

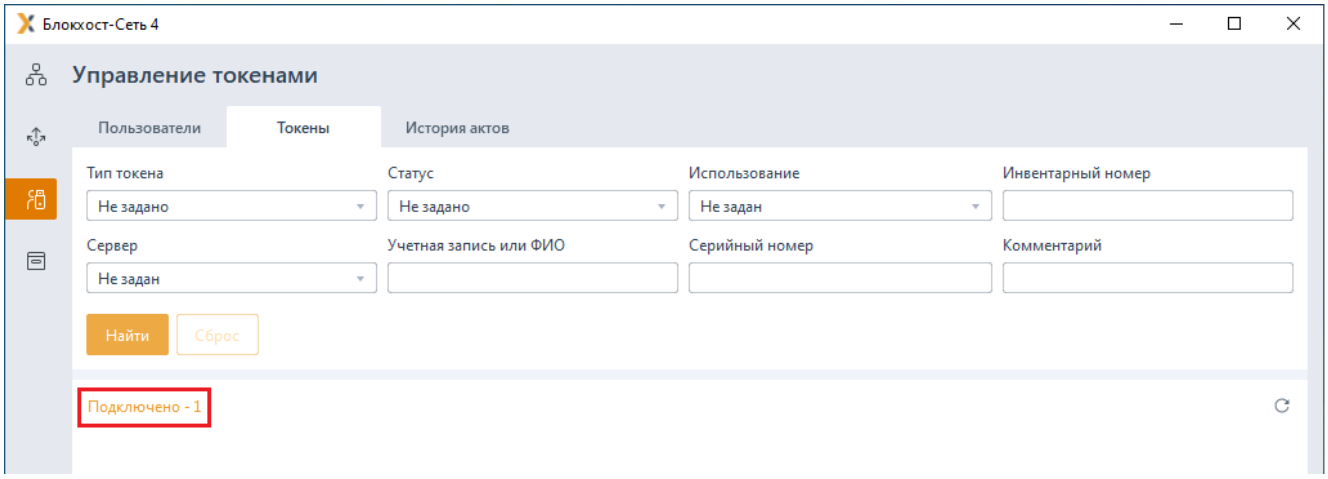


Рисунок 4.2 – Переход к подключенным устройствам

Не добавленный токен находится в состоянии ***Не зарегистрирован*** (рисунок 4.3).

Токен добавляется выбором в контекстном меню ***Зарегистрировать.***

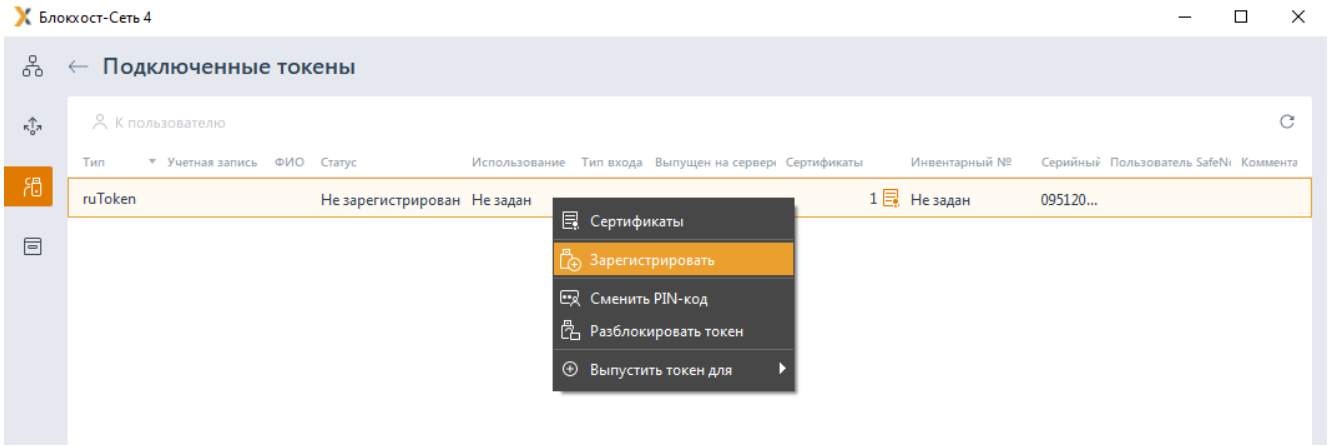


Рисунок 4.3 – Подключенные токены

В появившемся окне введите инвентарный номер токена и комментарий при необходимости (рисунок 4.4).

Поля ***Инвентарный номер*** и ***Комментарий*** не являются обязательными к заполнению и используются для облегчения учета и поиска токена в базе данных.

Наименование токена заполняется автоматически в соответствии с настройками, заданными для устройств (раздел ***«Настройка дополнительных параметров»***).

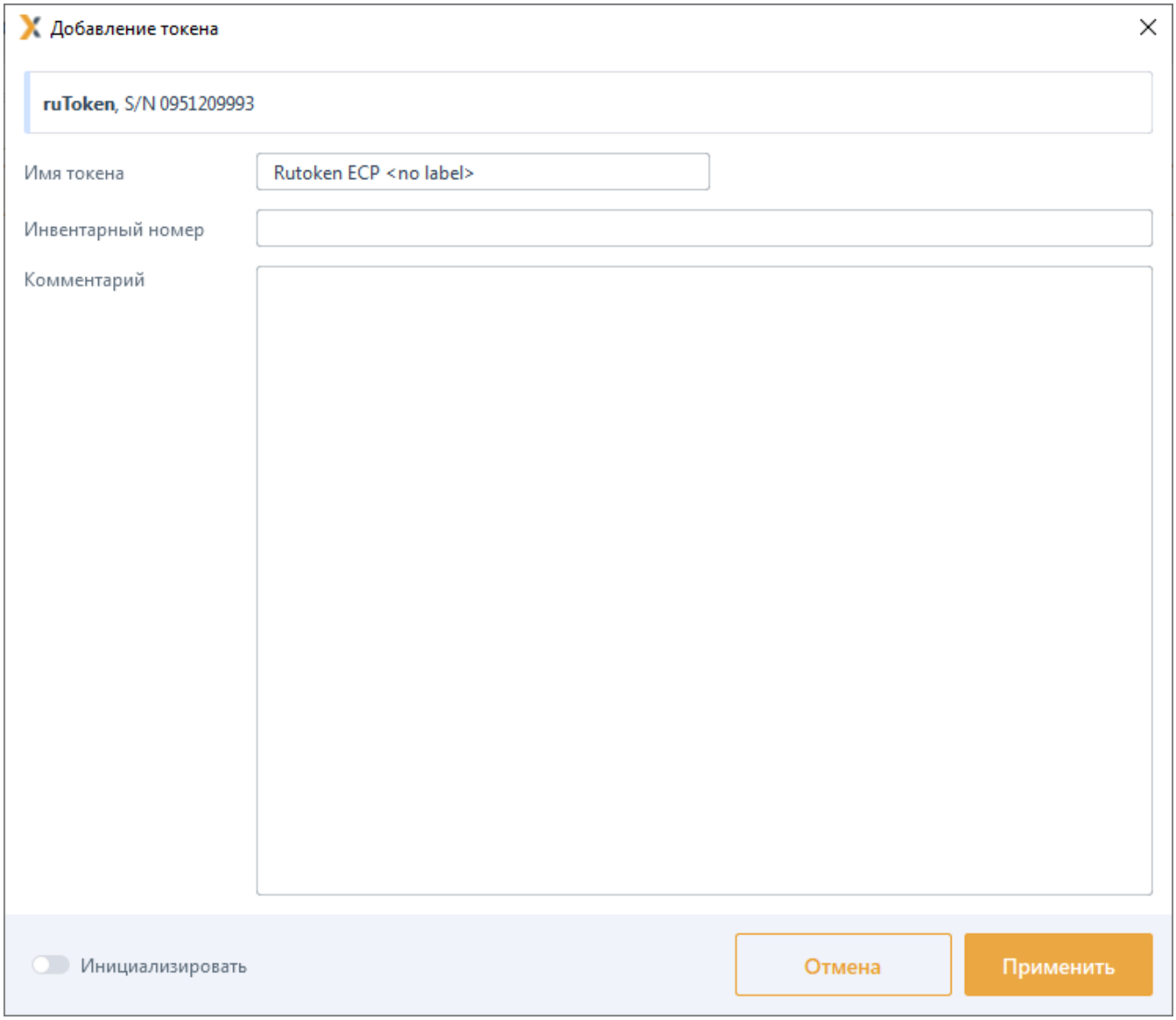


Рисунок 4.4 – Добавление токена

При включенной опции ***Инициализировать*** добавляемый токен будет инициализирован: все данные, хранимые на токене, удаляются, задаются новые значения PIN-кодов пользователя и администратора, и ограничения на них.

Установка параметров инициализации описана в разделе ***«Инициализация токена»***.

Добавленный токен, зарегистрированный в подсистеме, изменит состояние на ***Зарегистрирован*** (рисунок 4.5).

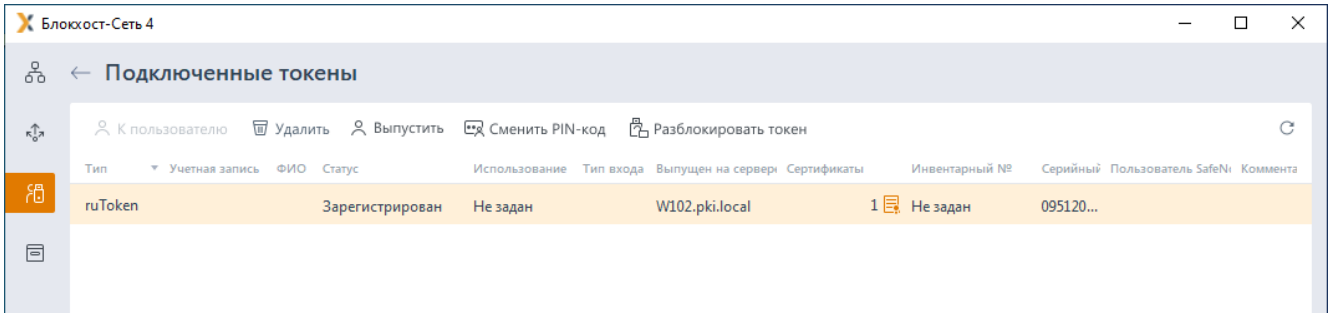


Рисунок 4.5 – Добавленный токен

4.2 Инициализация токена

Установка опции ***Инициализировать*** (рисунок 4.6) в процессе добавления токена позволяет выполнить инициализацию подключенного устройства.

При этом все хранимые на токене данные будут удалены.

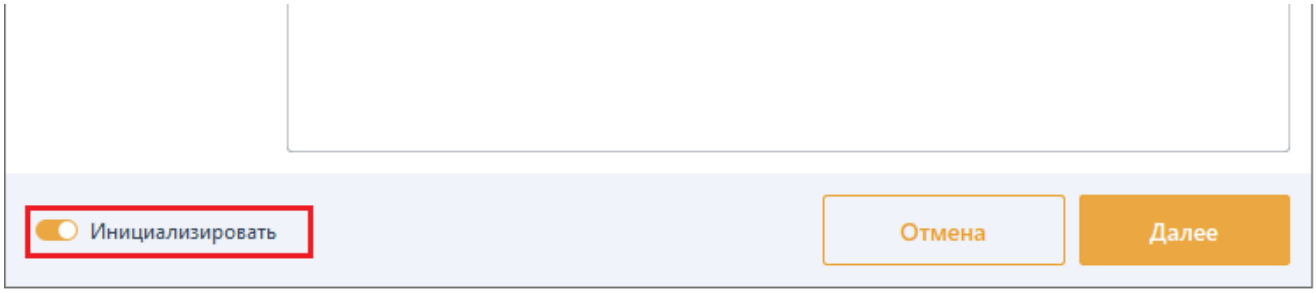


Рисунок 4.6 – Инициализация токена

Инициализация токена возможна двумя способами:

– с использованием профиля;

– без использования профиля (вручную).

4.2.1 Инициализация токена без использования профиля

В зависимости от типа устройства, для которого выполняется инициализация, параметры, доступные для изменения в окне ***Добавление токена***, будут различаться (рисунок 4.7).

Описание параметров инициализации каждого типа устройства приведено в разделе ***«Профили инициализации»***.

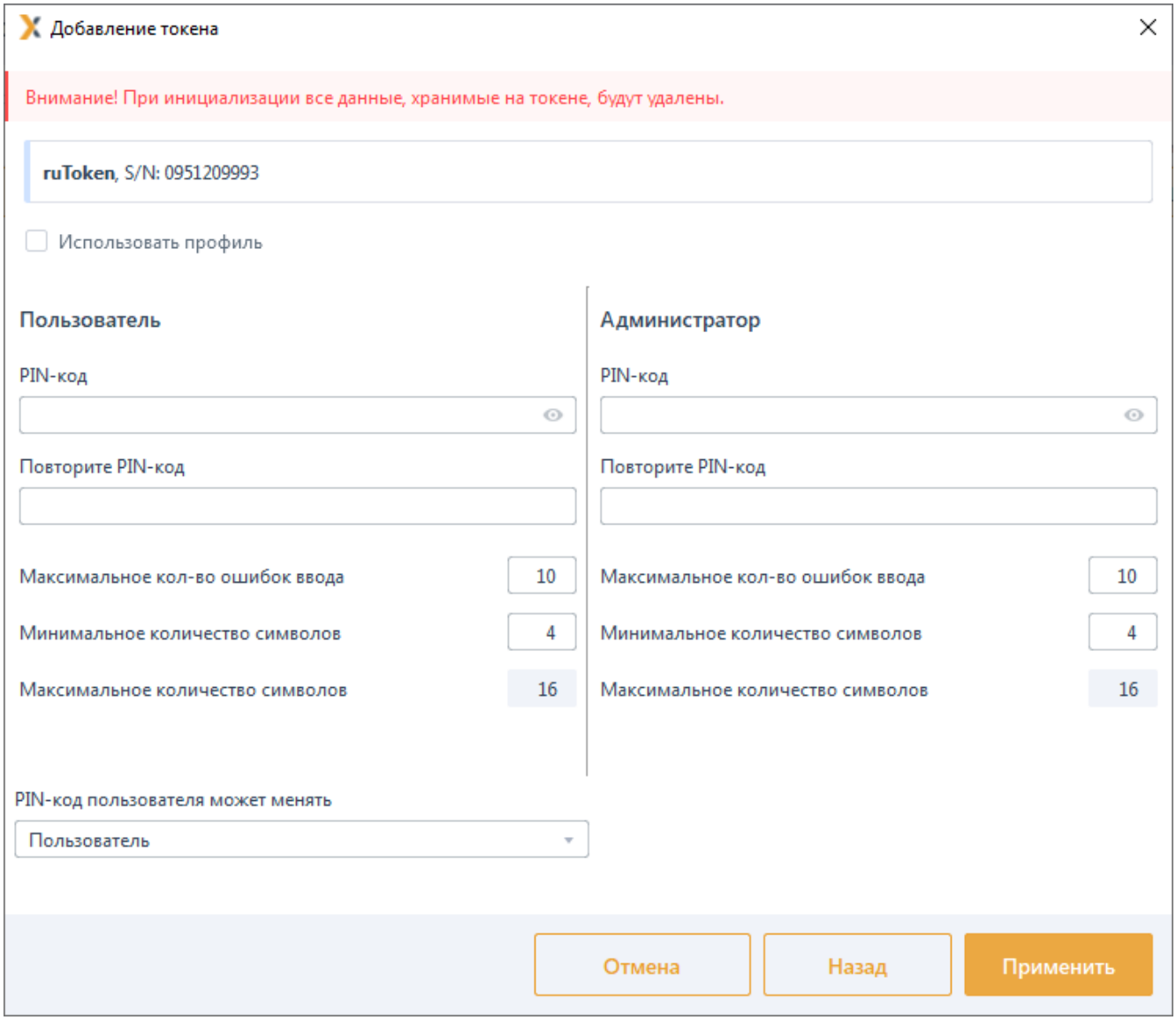


Рисунок 4.7 – Инициализация токена без использования профиля

После ввода необходимых параметров инициализации нажмите ***Применить*** для сохранения введенных параметров и выполнения инициализации.

4.2.2 Инициализация токена с использованием профиля

Установите опцию ***Использовать профиль*** (рисунок 4.8).

Выберите из списка нужный профиль.

Создание профилей инициализации описано в разделе ***«Профили инициализации»***.

Нажмите ***Применить***.

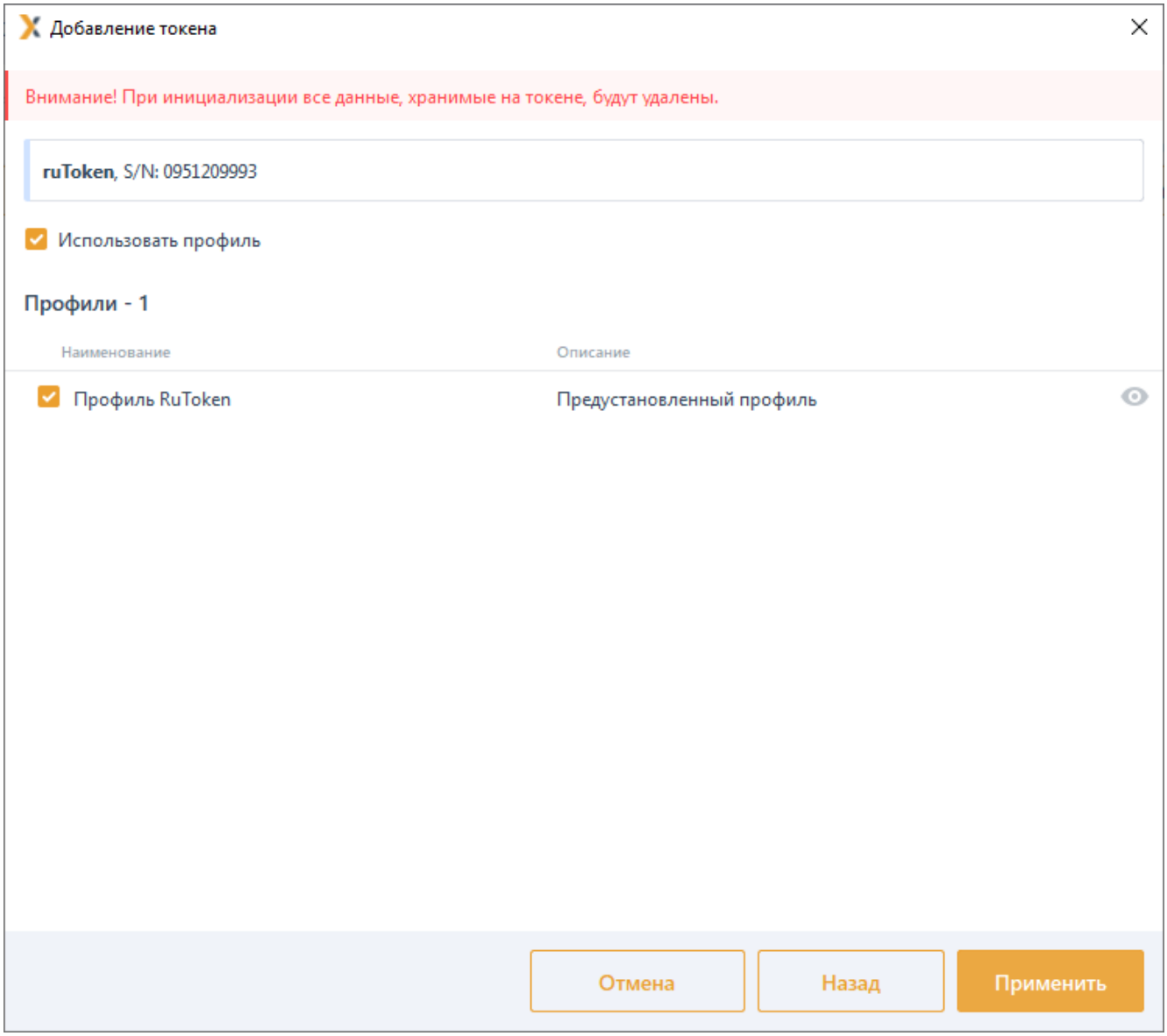


Рисунок 4.8 – Выбор профиля

4.3 Профили инициализации

При инициализации устройства в процессе добавления токена возможно использование профилей инициализации.

Профили инициализации позволяют настроить параметры инициализации для каждого типа устройств, поддерживаемого подсистемой жизненного цикла токенов, и при последующей инициализации токена использовать профиль для выбранного устройства.

Для создания профилей инициализации перейдите в раздел ***«Профили инициализации»*** по кнопке (рисунок 4.9).

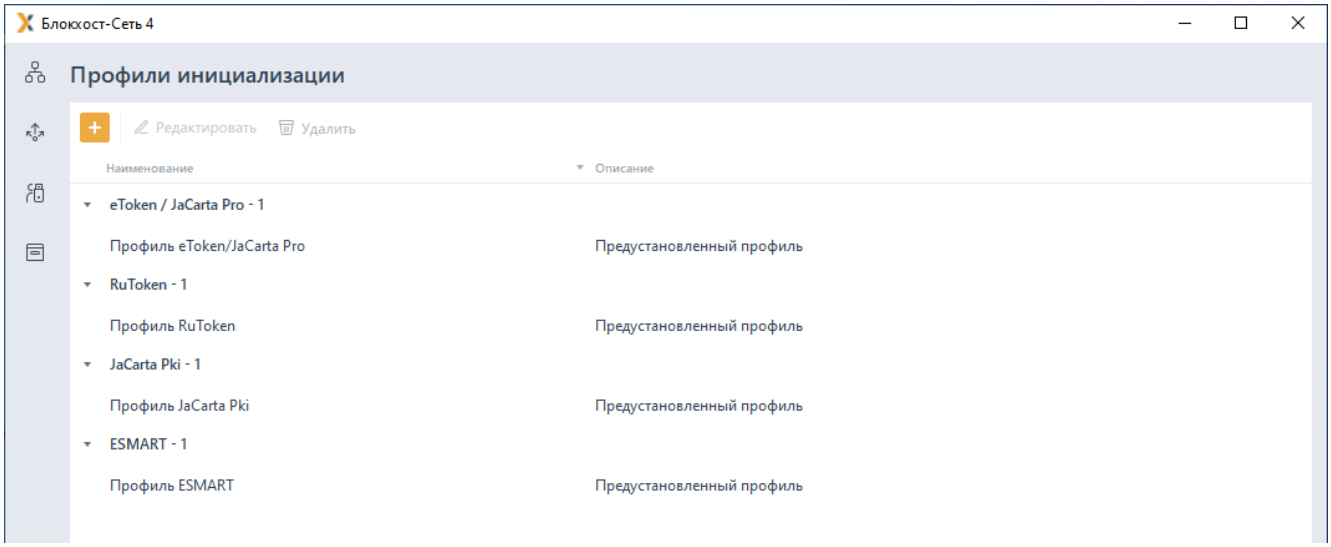


Рисунок 4.9 – Создание профилей инициализации

По кнопке  выберите тип устройства, для которого создается профиль (рисунок 4.10).

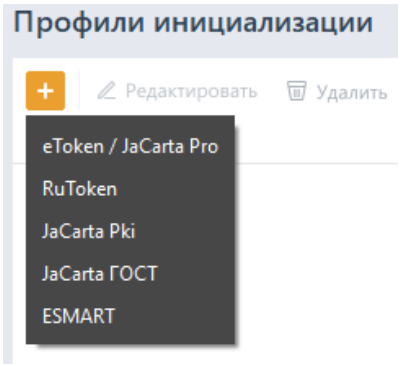


Рисунок 4.10 – Выбор типа устройства

В зависимости от выбранного типа устройства, параметры, доступные для изменения в окне ***Создание профиля инициализации устройств для <наименование устройства>***, будут различаться (рисунок 4.11).

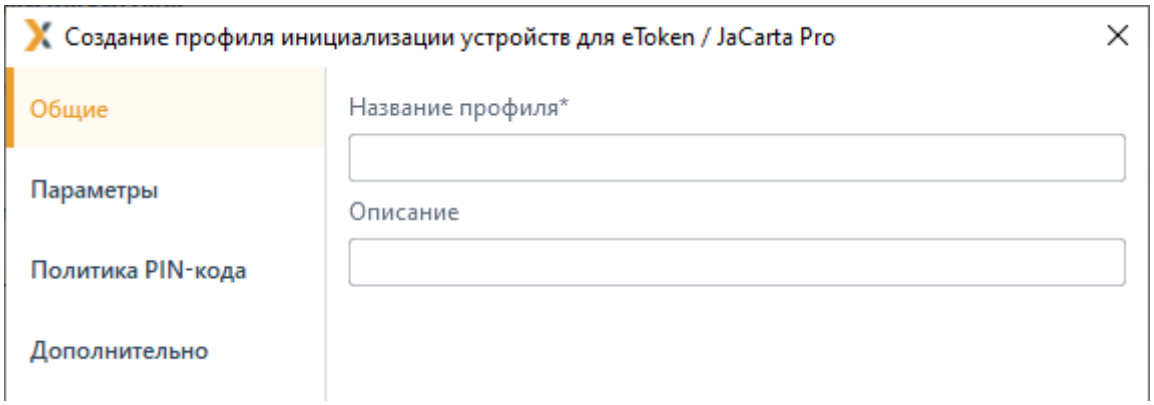


Рисунок 4.11 – Создание профиля инициализации для выбранного устройства

Вкладка ***Общие*** (рисунок 4.11) содержит общие для всех типов устройств параметры:

– название для создаваемого профиля;

– описание профиля (при необходимости).

Во вкладке ***Параметры*** (рисунок 4.12) задаются параметры:

– PIN-код доступа для пользователя и администратора;

– максимально разрешенное количество ошибок при вводе пароля для пользователя и администратора;

– минимально допустимое количество символов при создании пароля;

– максимально допустимое количество символов при создании пароля (для устройств JaCarta PKI);

– возможность изменять PIN-код пользователя администратору и/или пользователю (для устройств Рутокен).

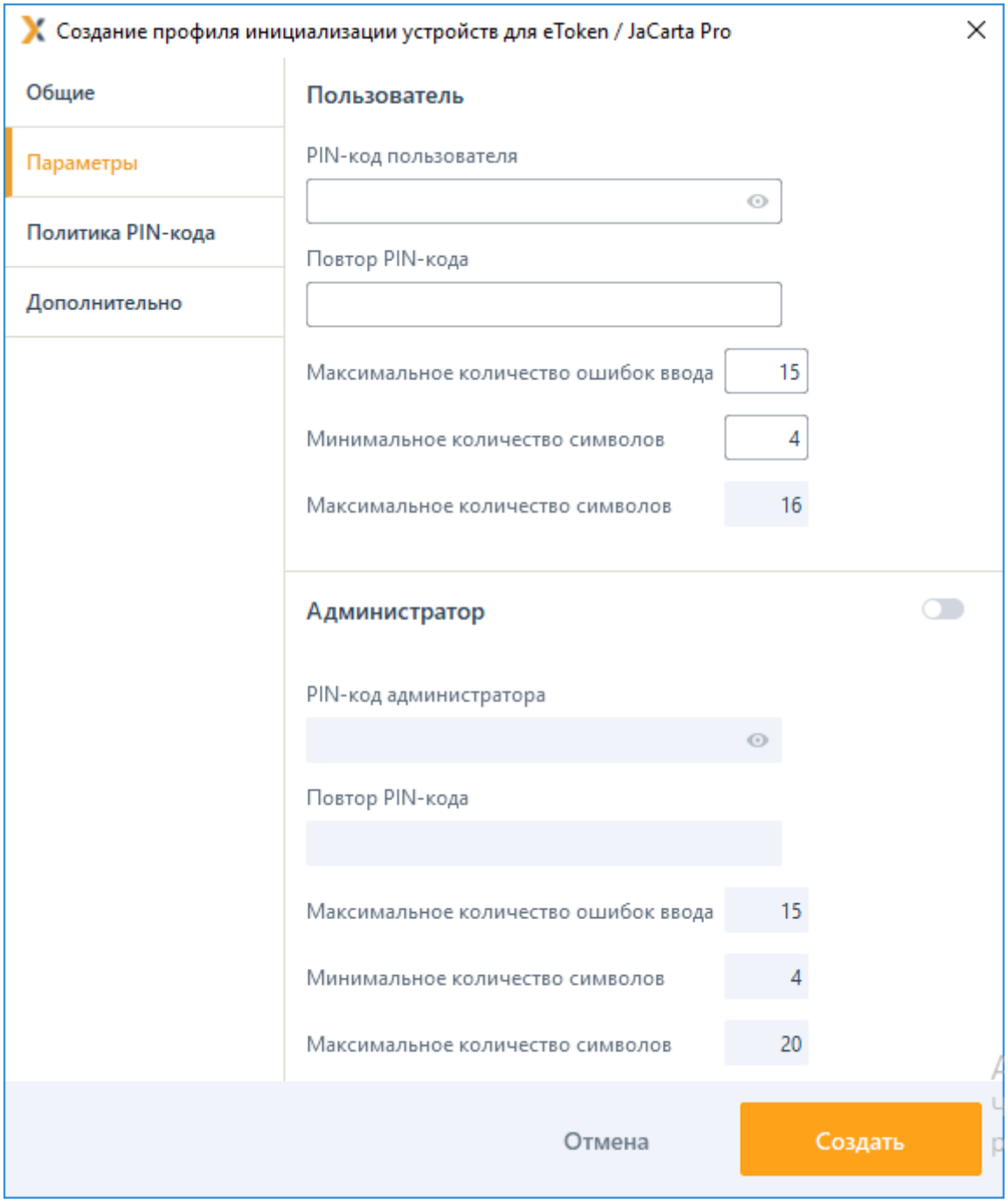


Рисунок 4.12 – Вкладка ***Параметры***

Во вкладке ***Политика PIN-кода*** (рисунок 4.13) задаются параметры:

– для устройств eToken/JaCarta Pro:

- минимальный/максимальный срок действия PIN-кода пользователя;
- количество дней, за которое необходимо предупредить пользователя об окончании срока действия пароля;
- количество PIN-кодов пользователя, хранящихся в памяти подсистемы и

недоступных для повторного использования пользователем;

- символы, допустимые или обязательные к использованию при создании PIN-кода пользователя (числовые, в верхнем регистре, в нижнем регистре, специальные) и максимально возможное последовательное повторение используемых символов;

– для устройств JaCarta PKI:

- минимальное число символов, используемых при создании PIN-кода администратора и пользователя (числовых, в верхнем регистре, в нижнем регистре, специальных) и максимально возможное последовательное повторение используемых символов.

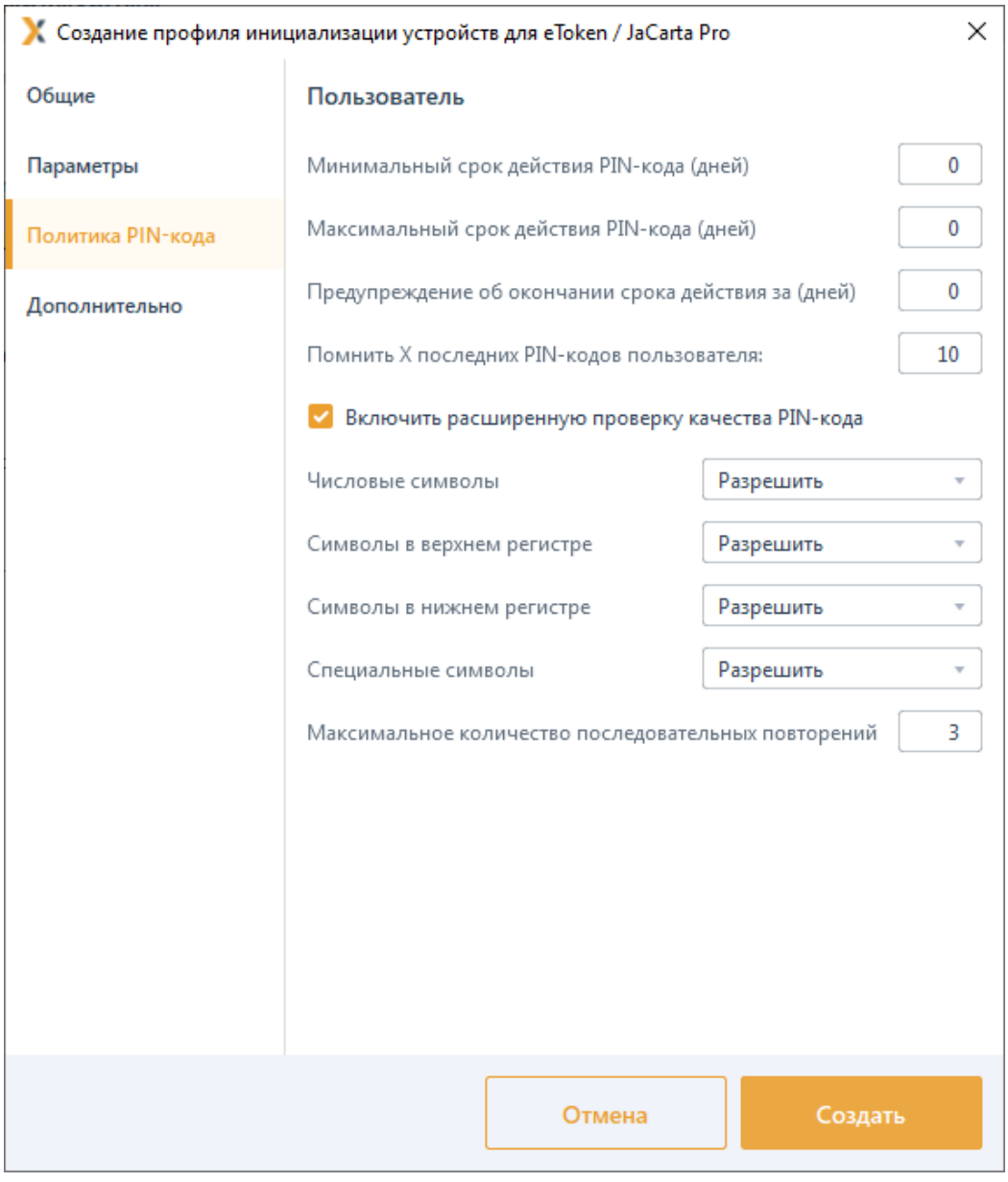


Рисунок 4.13 – Вкладка ***Политика PIN-кода***

Во вкладке ***Дополнительно*** (для устройств eToken/JaCarta Pro) задается частота кеширования приватных данных (рисунок 4.14).

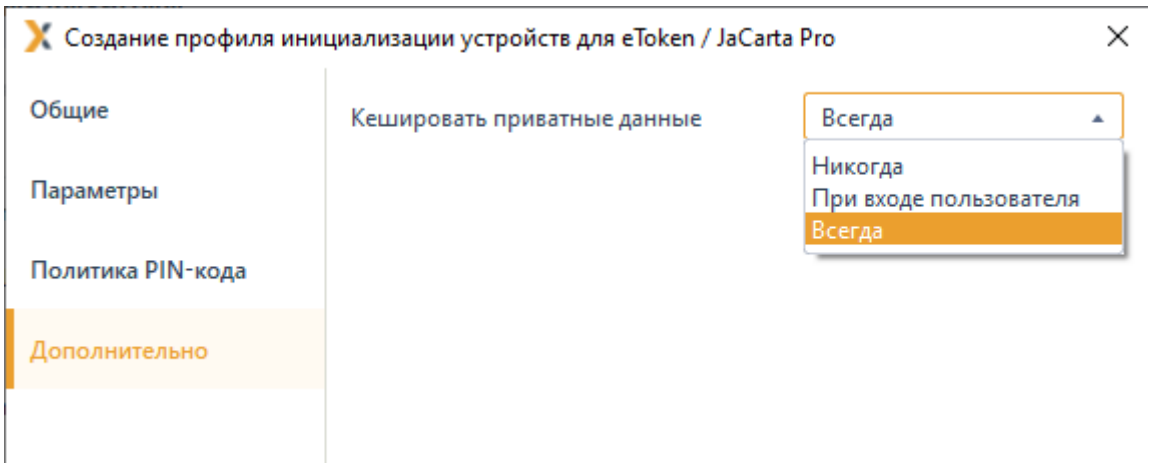


Рисунок 4.14 – Вкладка ***Дополнительно***

В дальнейшем при инициализации токена установите опцию ***Использовать профиль*** и выберите из списка один из добавленных профилей (рисунок 4.15).

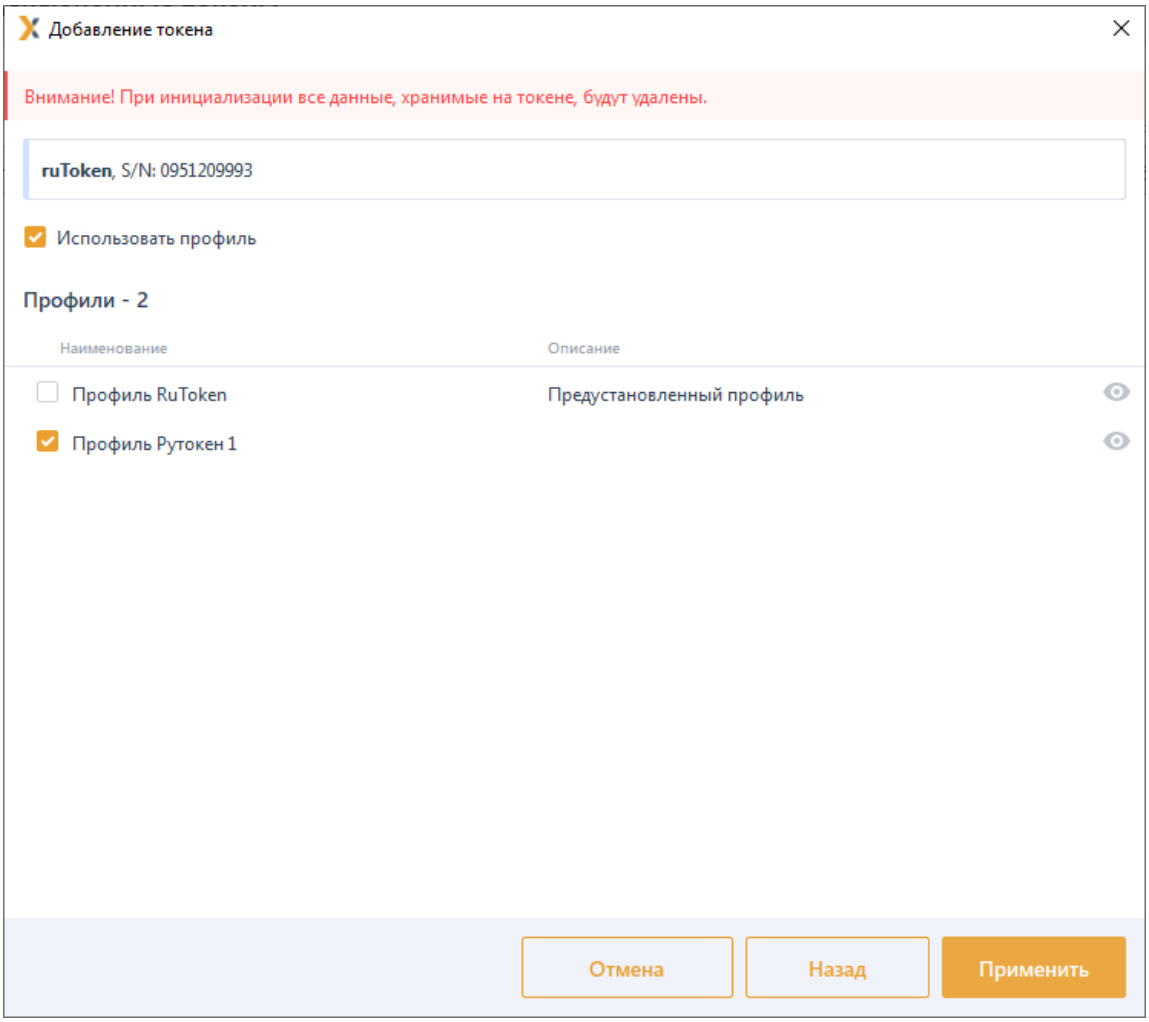


Рисунок 4.15 – Использование профиля инициализации

4.4 Поиск токена

Поиск токена применяется в случае, если известны некоторые параметры устройства (тип токена, инвентарный и/или серийный номер, состояние токена, пользователь).

Для поиска токена перейдите во вкладку ***Токены***.

Введите один или несколько параметров устройства (рисунок 4.16).

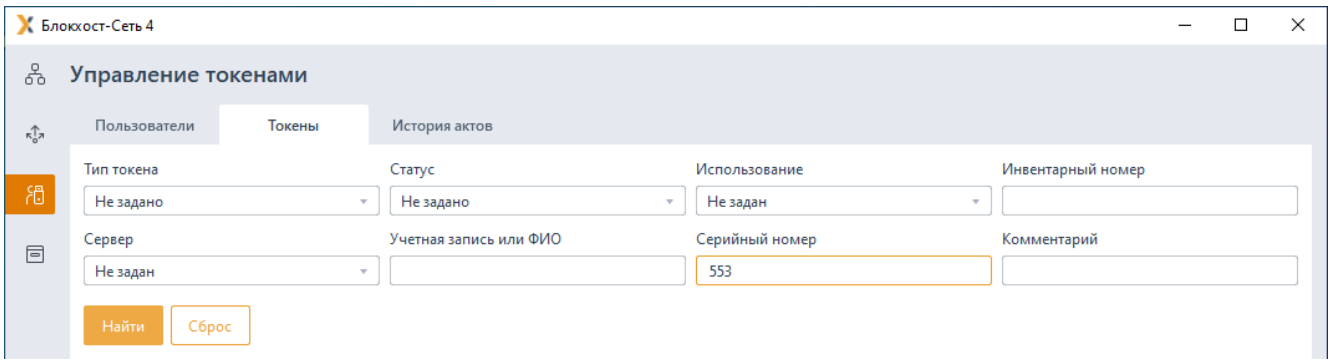


Рисунок 4.16 – Ввод параметров поиска

Нажмите кнопку ***Найти***.

Кнопка ***Сброс*** предназначена для отмены всех введенных параметров поиска.

В списке отобразятся все устройства, удовлетворяющие введенным параметрам (рисунок 4.17).

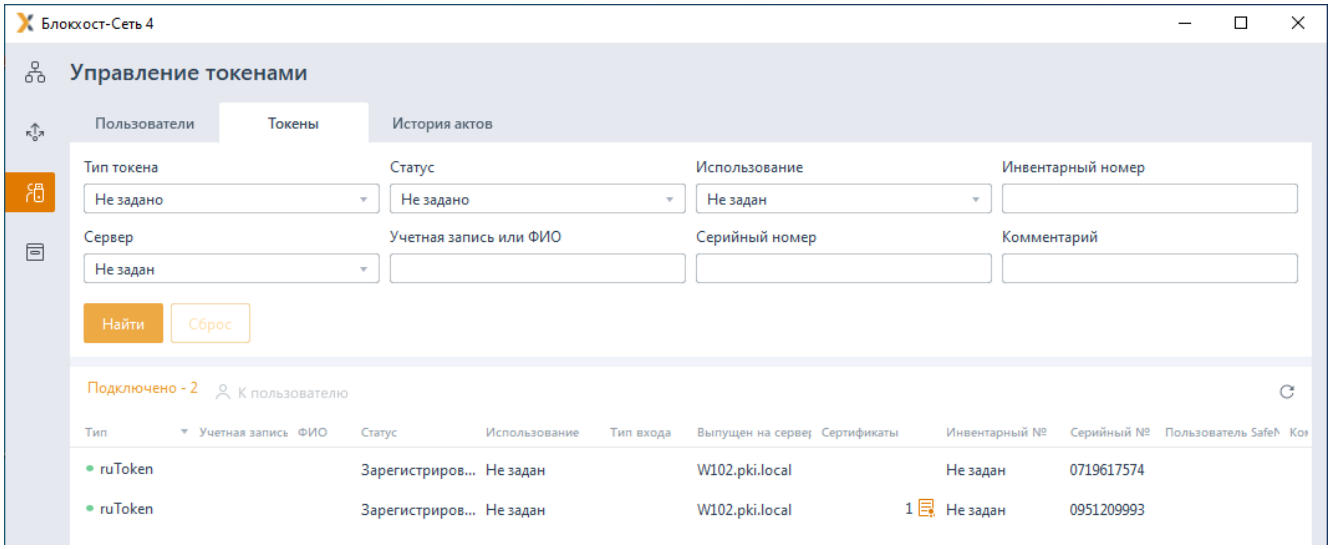


Рисунок 4.17 – Поиск устройств

Максимально возможное количество токенов, отображаемых в результатах поиска – 20. При отсутствии необходимого токена в списке, укажите более точные параметры поиска.

4.5 Удаление токена

Удаление токена из подсистемы возможно, как при наличии подключенного к АРМ администратора безопасности устройства, так и без него.

Удалить можно только токен, не назначенный пользователю, в состоянии ***Зарегистрирован***.

Для удаления токена выполните его поиск по известным параметрам во вкладке ***Токены***.

Перейдите в строку с токеном, который необходимо удалить из подсистемы.

Выберите в контекстном меню ***Удалить из системы*** (рисунок 4.18).

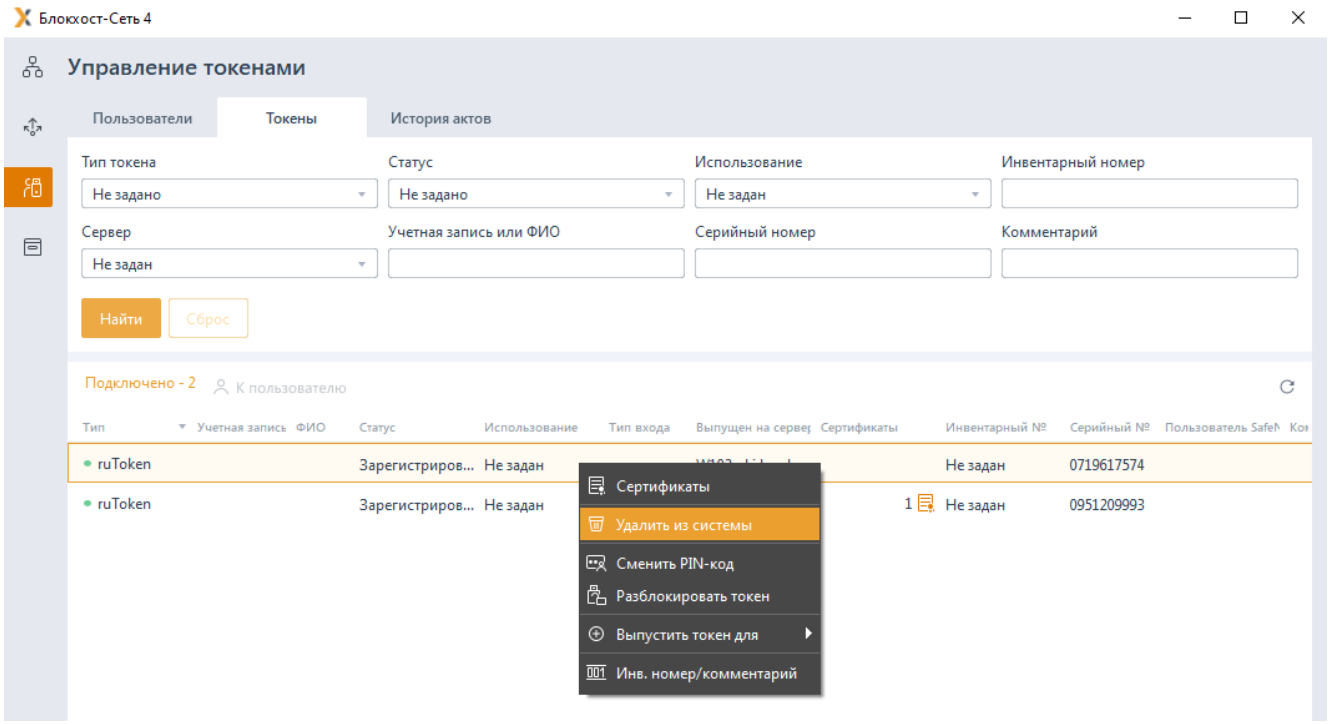


Рисунок 4.18 – Удаление токена из подсистемы

Удаленный токен возможно повторно зарегистрировать в подсистеме во вкладке ***Подключенные токены***, подключив устройство к компьютеру.

При выполнении операции удаления токена возможно формирование акта ***«Уничтожение токена»***. Настройка формирования акта при выполнении операции удаления осуществляется во вкладке ***Настройки*** в разделе ***«Шаблоны печати»*** путем установки или снятия флага напротив акта (подробнее в разделе ***«Шаблоны печати»***).

Возможность распечатать акт, формируемый при удалении токена из системы доступна не только в момент выполнения операции, но и по прошествии времени во вкладке ***История актов*** (подробнее в разделе **История актов**).

4.6 Просмотр сертификатов на токене

Просмотр сертификатов на токене доступен только при наличии подключенного к АРМ администратора безопасности устройства.

Для просмотра сертификатов на токене выполните его поиск по известным параметрам во вкладке ***Токены,*** либо перейдите по ссылке ***Подключено*** в окно ***Подключенные токены***.

Перейдите в строку с токеном, на котором необходимо просмотреть сертификаты.

Выберите в контекстном меню ***Сертификаты*** (рисунок 4.19).

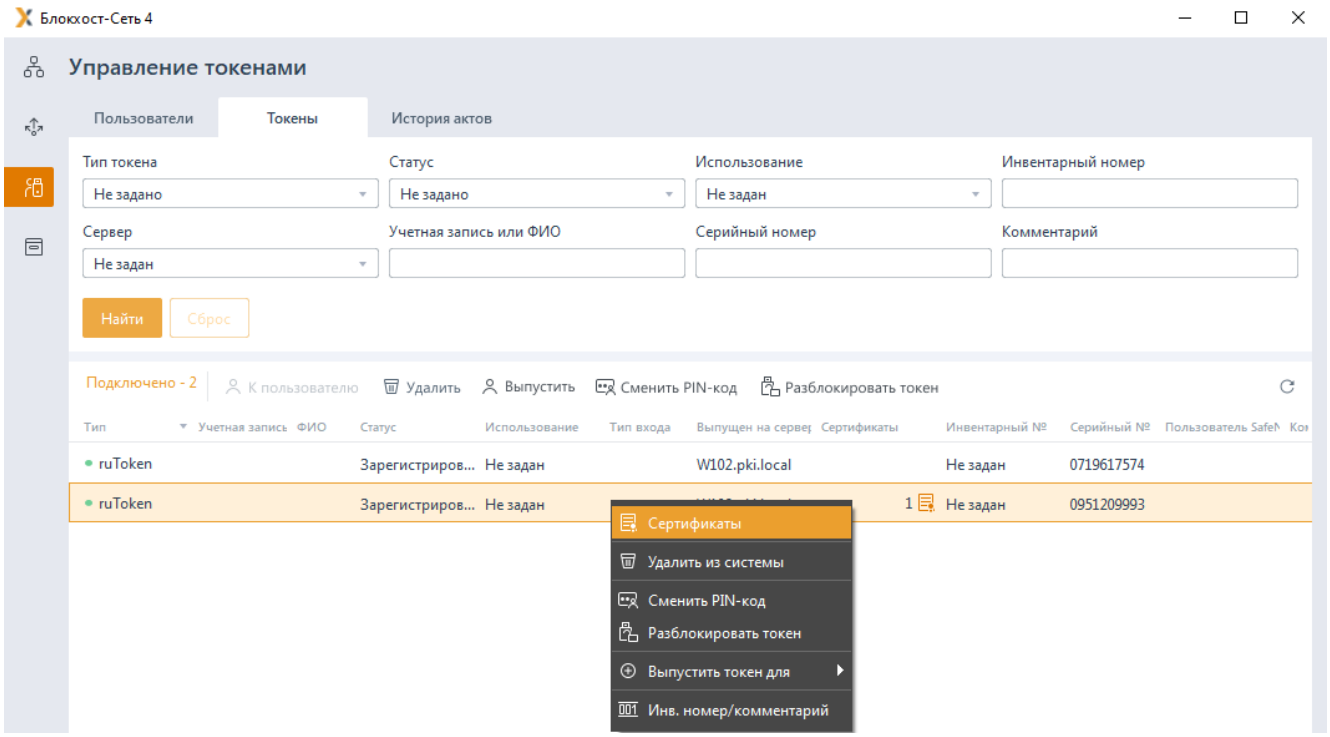


Рисунок 4.19 – Просмотр сертификатов на токене

В появившемся окне отобразятся все сертификаты, находящиеся на выбранном токене (рисунок 4.20).

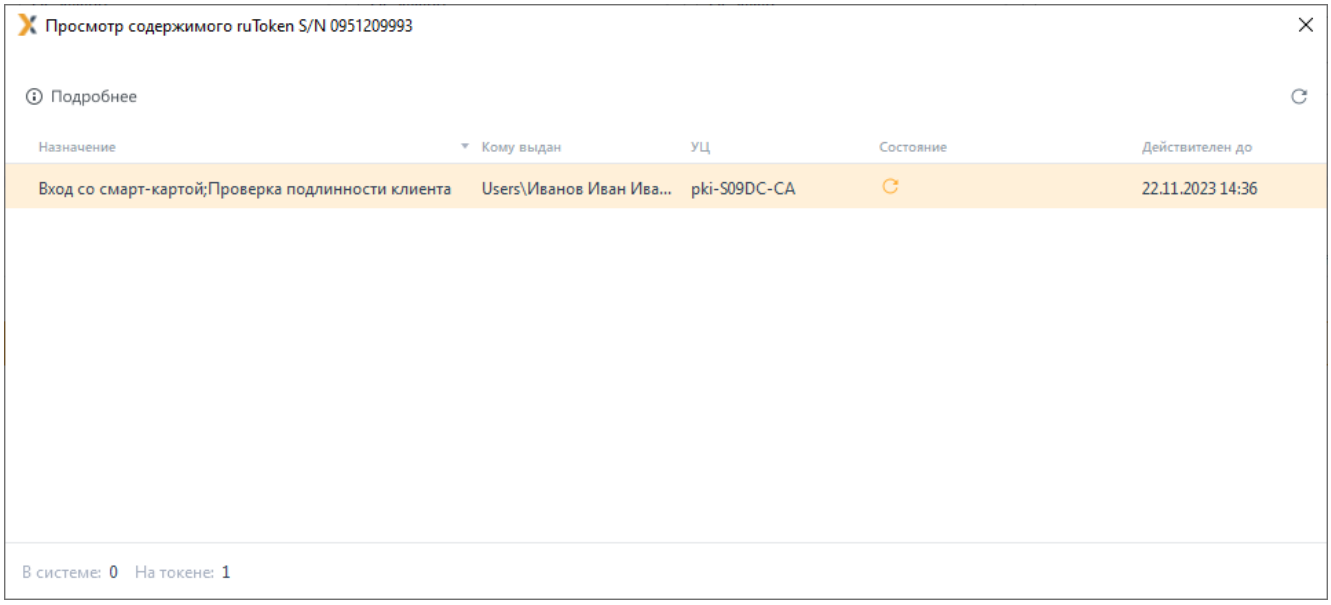


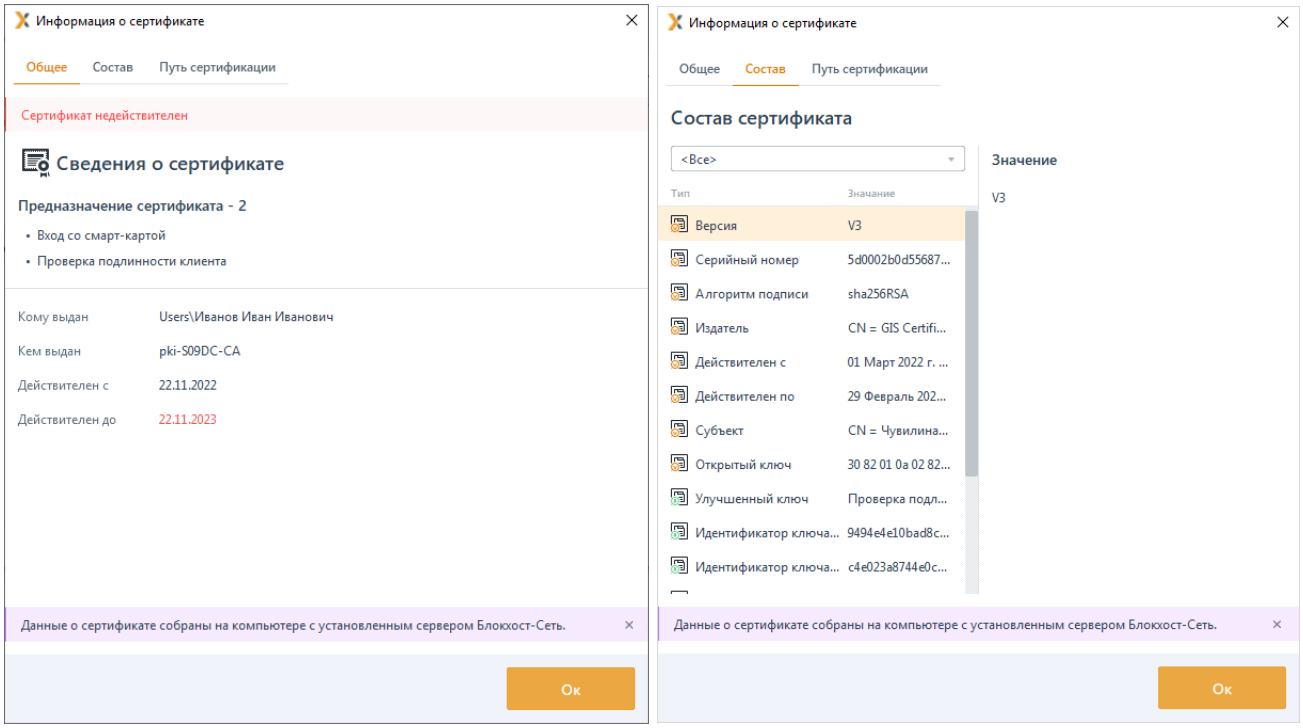
Рисунок 4.20 – Сертификаты на выбранном токене

При нажатии на кнопку Подробнее появится окно, содержащее расширенную информацию в сертификате (рисунок 4.21):

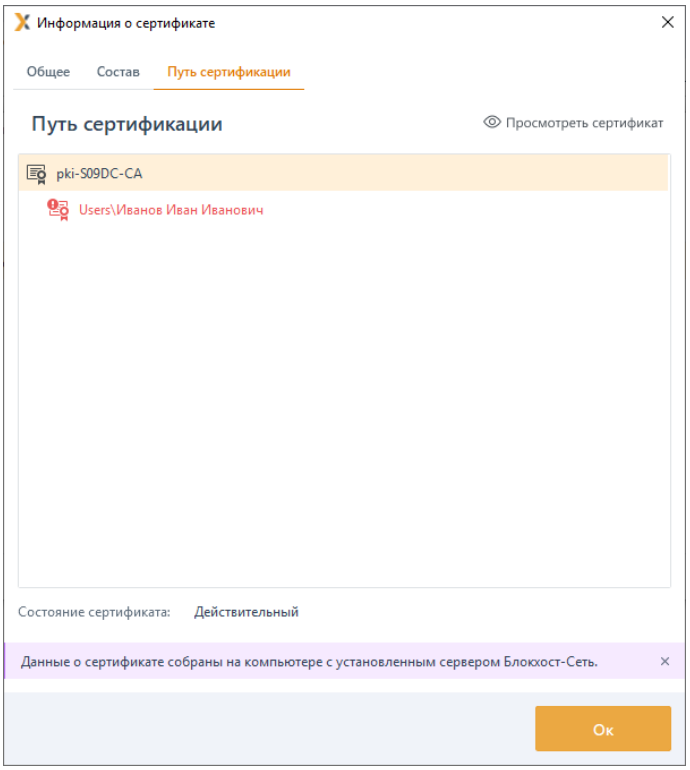
– на вкладке ***Общее*** отображаются сведения о сертификате, его назначение, кому и кем выдан сертификат и срок его действия;

– на вкладке ***Состав*** отображаются сведения о составе сертификата, его поля, расширения и свойства;

– на вкладке ***Путь сертификации*** отображаются сведения о цепочке сертификации.



а) б)



в)

Рисунок 4.21 – Подробные сведения о сертификатах на выбранном токене

При отсутствии сертификатов на токене или извлечении токена появится сообщение:

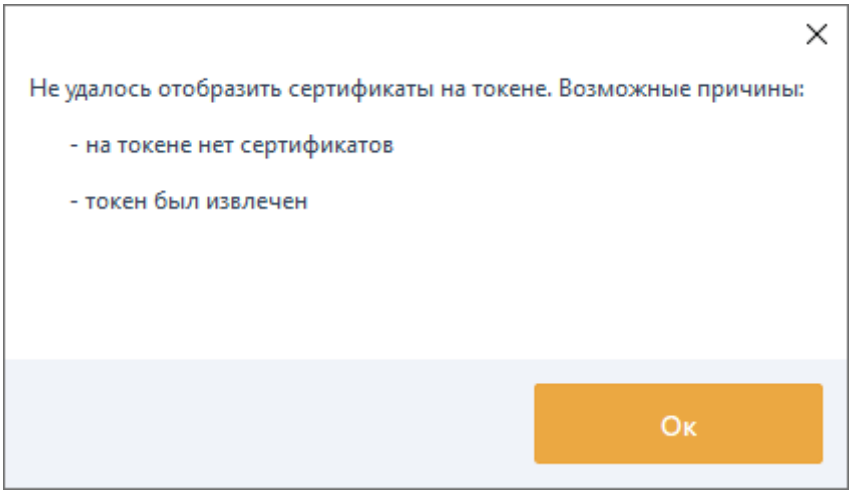


Рисунок 4.22 – Ошибка при просмотре сертификатов на токене

4.7 Смена PIN-кода токена

Для изменения PIN-кода пользователя на токене выполните поиск по пользователю, либо выполните его поиск по известным параметрам во вкладке ***Токены,*** либо перейдите по ссылке ***Подключено*** в окно ***Подключенные токены***.

Перейдите в строку с токеном, на котором необходимо сменить PIN-код.

Выберите в контекстном меню ***Сменить PIN-код*** (рисунок 4.23).

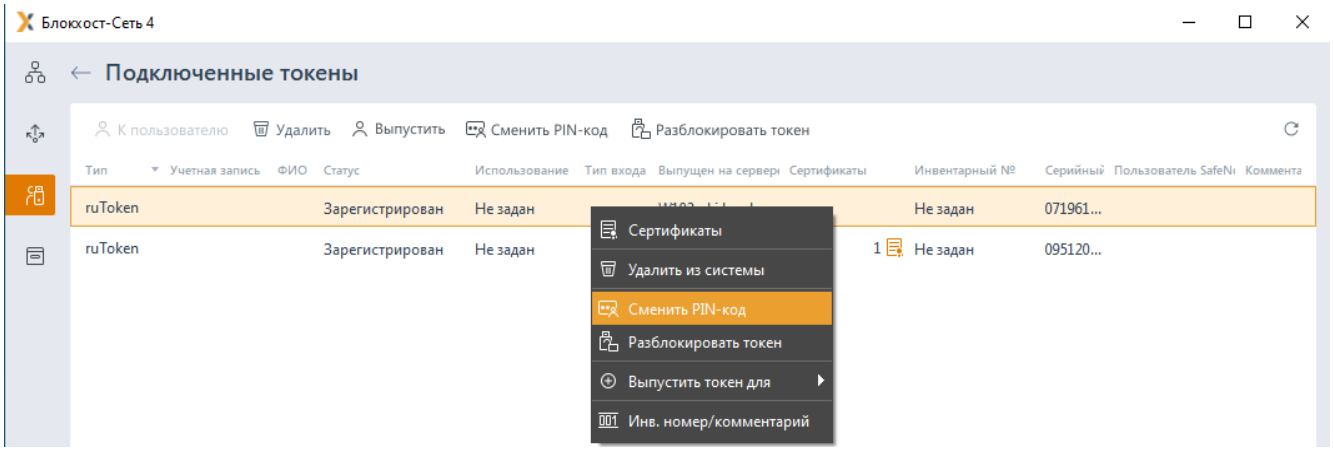


Рисунок 4.23 – Смена PIN-кода пользователя

В появившемся окне введите PIN-код администратора и измените PIN-код пользователя (рисунок 4.24).

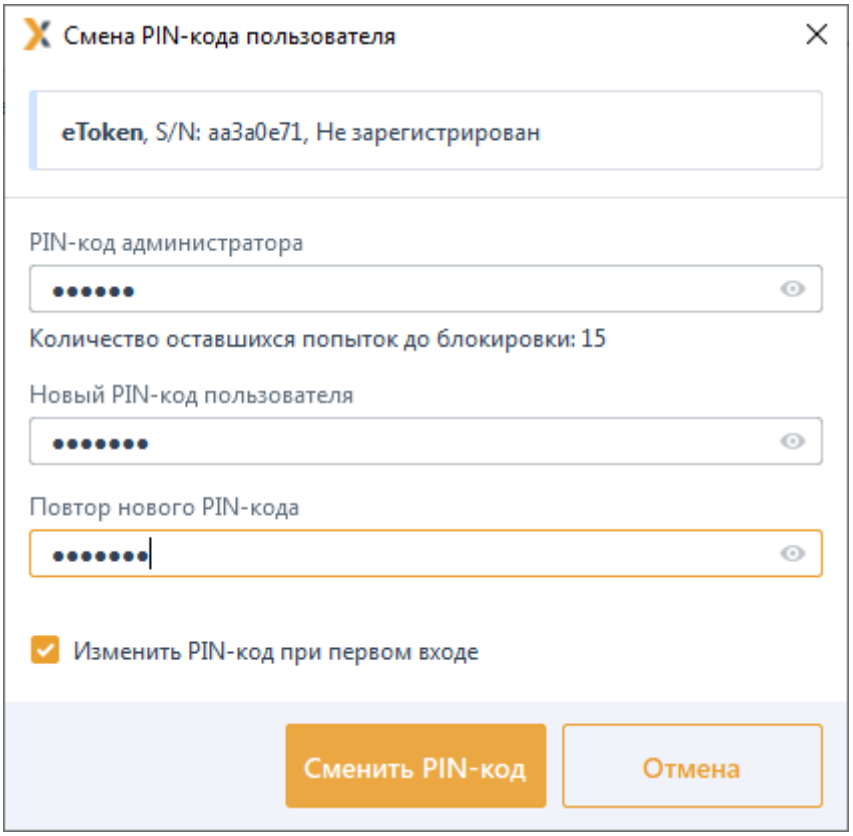


Рисунок 4.24 – Ввод нового PIN-кода пользователя

После смены PIN-кода пользователь сможет входить на токен с использованием нового PIN-кода.

Если смена PIN-кода пользователя выполняется после превышения количества неудачных попыток входа пользователем на токен, при смене PIN-кода токен будет разблокирован (рисунок 4.25).

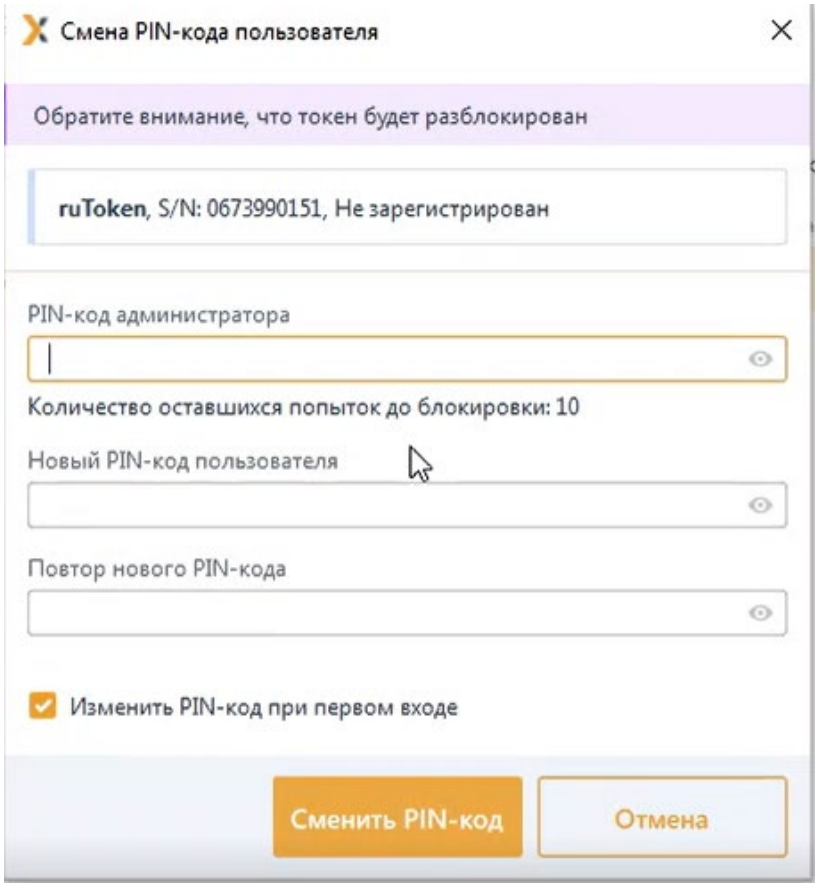


Рисунок 4.25 – Смена PIN-кода пользователя и разблокировка токена

При операции смены PIN-кода пользователя последовательность запрашиваемых действий может быть различна в зависимости от типа используемого токена (таблица 4.1).

Таблица 4.1 – Запрашиваемые действия при смене PIN-кода токена

Смена PIN-кода токена			
	Токен заблокирован	**Токен разблокирован**	**Примечание**
Рутокен	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется.	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается.	Смена PIN-кода возможна, только если на токене включено разрешение на смену PIN-кода пользователя администратором (иначе токен выдаст ошибку)

	Дополнительно: Появляется сообщение, что токен будет разблокирован		
Etoken	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что токен будет разблокирован	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается.	Смена PIN-кода возможна, только если при инициализации токена был задан PIN-код администратора (иначе токен выдаст ошибку)
Jacarta PKI	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что токен будет разблокирован	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается.	
JaCarta Pro	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат:	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат:	

	• смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что токен будет разблокирован	• смена PIN-кода пользователя; • счетчик попыток сбрасывается.	
Esmart	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что токен будет разблокирован	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается.	

4.8 Разблокировка токена

Для изменения разблокировки токена выполните поиск по пользователю, либо выполните его поиск по известным параметрам во вкладке ***Токены,*** либо перейдите по ссылке ***Подключено*** в окно ***Подключенные токены***.

Перейдите в строку с токеном, который необходимо разблокировать.

Выберите в контекстном меню ***Разблокировать токен*** (рисунок 4.26).

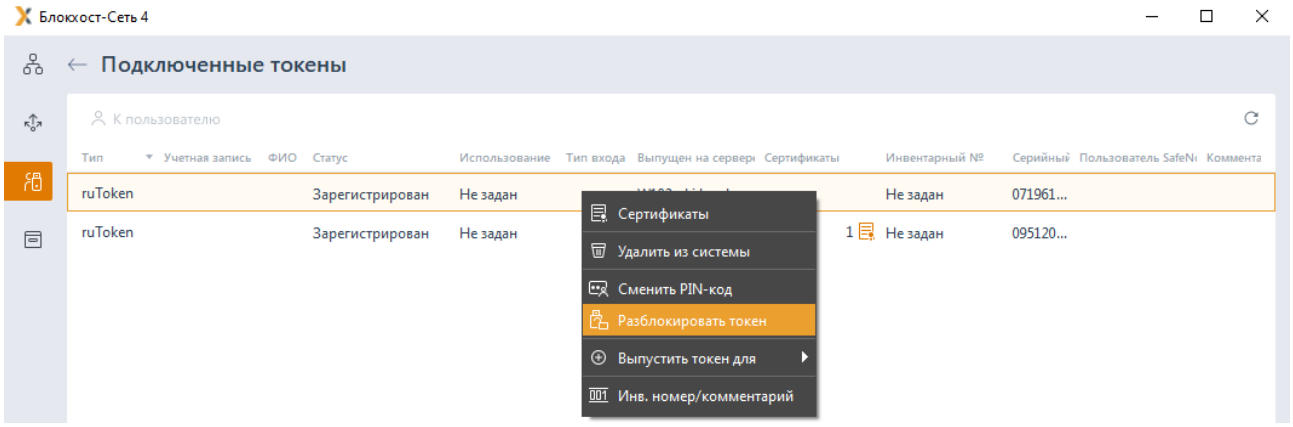


Рисунок 4.26 – Контекстное меню токена

В появившемся окне введите PIN-код администратора и нажмите кнопку ***Разблокировать*** (рисунок 4.27).

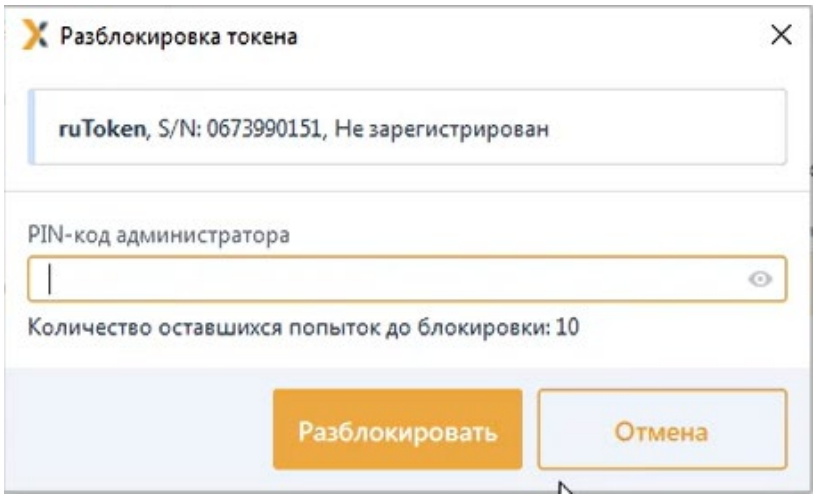


Рисунок 4.27 – Разблокировка токена

После разблокировки токена пользователь сможет входить на токен с использованием прежнего PIN-кода.

При операции разблокировки токена пользователя последовательность запрашиваемых действий может быть различна в зависимости от типа используемого токена (таблица 4.2).

Таблица 4.2 – Запрашиваемые действия при разблокировке токена

Разблокировка токена		
	Токен заблокирован	**Токен разблокирован**
Рутокен	Входные данные: • PIN-код администратора. Ожидаемый результат: • счетчик попыток сбрасывается;	Сообщение об ошибке: «Операция не поддерживается, т.к. токен не заблокирован».

	• токен разблокируется.	
Etoken	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что для разблокировки токена необходимо сменить PIN-код пользователя	Сообщение об ошибке: «Операция не поддерживается, т.к. токен не заблокирован».
Jacarta PKI	Входные данные: • PIN-код администратора, • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • счетчик попыток сбрасывается; токен разблокируется.	Сообщение об ошибке: «Операция не поддерживается, т.к. токен не заблокирован».
JaCarta Pro	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется. Дополнительно: Появляется сообщение, что для разблокировки токена необходимо сменить PIN-код пользователя	Сообщение об ошибке: «Операция не поддерживается, т.к. токен не заблокирован».
Esmart	Входные данные: • PIN-код администратора, новый PIN-код пользователя; • требование смены PIN-кода пользователя при первом входе в ОС. Ожидаемый результат: • смена PIN-кода пользователя; • счетчик попыток сбрасывается; • токен разблокируется.	Сообщение об ошибке: «Операция не поддерживается, т.к. токен не заблокирован».

	Дополнительно: Появляется сообщение, что для разблокировки токена необходимо сменить PIN-код пользователя	

4.9 Инвентарный номер/Комментарий

Для изменения инвентарного номера токена или добавления комментария выполните поиск токена по известным параметрам во вкладке ***Токены,*** либо перейдите по ссылке ***Подключено*** в окно ***Подключенные токены***.

Перейдите в строку с токеном, на котором необходимо изменить инвентарный номер.

Выберите в контекстном меню ***Инв. номер/комментарий*** (рисунок 4.28).

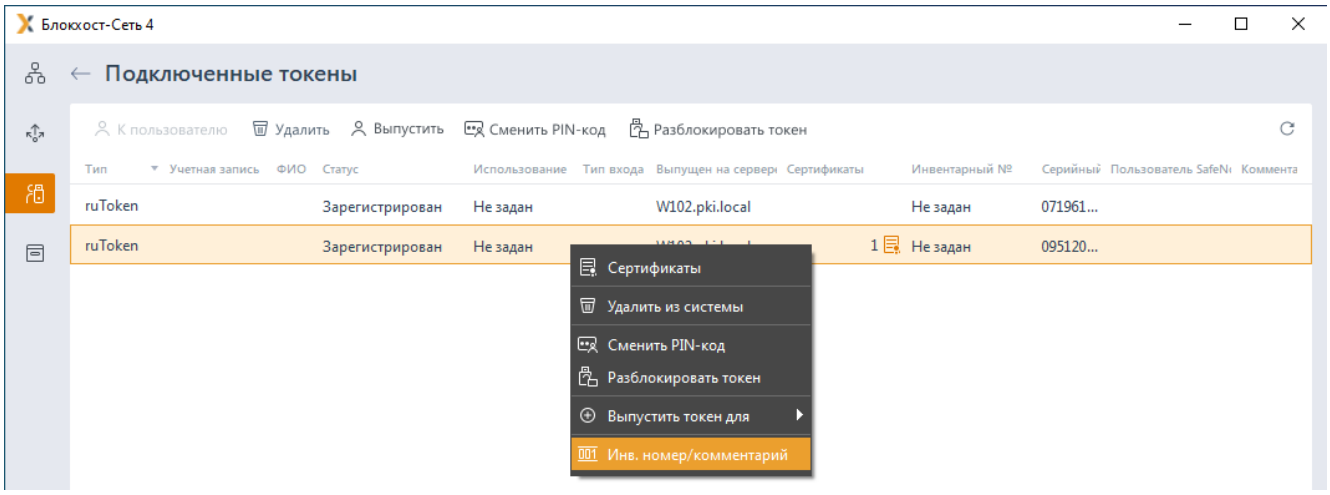


Рисунок 4.28 – Инвентарный номер/Комментарий

В появившемся окне измените инвентарный номер выбранного токена или добавьте комментарий при необходимости (рисунок 4.29).

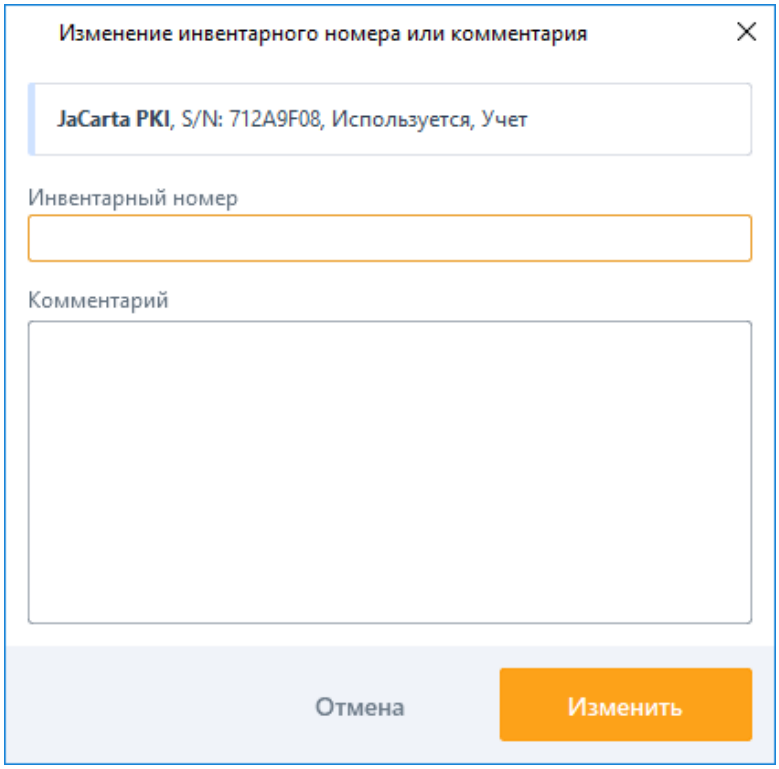


Рисунок 4.29 – Изменение инвентарного номера токена

Для сохранения введенных параметров нажмите ***Изменить***.

4.10 Выпуск токена

Выпуск токена пользователю заключается в привязке устройства конкретному пользователю.

Выпуск токена пользователю доступен только в состояниях ***Не зарегистрирован*** и ***Зарегистрирован***.
Выпуск токена доступен только при наличии устройства.

Возможен выпуск токена пользователю:

– для входа по управляемому сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный средствами подсистемы управления токенами);

– для входа по стороннему сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный сторонними средствами);

– для безопасного входа по паролю (при использовании токена для аутентификации по паролю, записанному на устройство);

– для учета сертификатов, находящихся на токене (взятие сертификатов на токене,

выпущенных УЦ сторонних организаций, под наблюдение).

Описание выпуска токена пользователю приведено в разделе ***«Назначение токена пользователю».***

При выполнении операции выпуска токена возможно формирование акта ***«Прием-передача токена в эксплуатацию»***. Настройка формирования акта при выполнении операции выпуска токена осуществляется во вкладке ***Настройки*** в разделе ***«Шаблоны печати»*** путем установки или снятия флага напротив акта (подробнее в разделе ***«Шаблоны печати»***).

Возможность распечатать акт, формируемый при выпуске токена пользователю доступна не только в момент выполнения операции, но и по прошествии времени во вкладке ***История актов*** (подробнее в разделе ***«История актов»***).

4.11 История актов

Во вкладке ***История актов*** хранятся все акты, сформированные пользователями, осуществляется поиск актов по заданным параметрам с возможностью сохранения требуемых актов в нужной директории или на внешний носитель информации (рисунок 4.30).

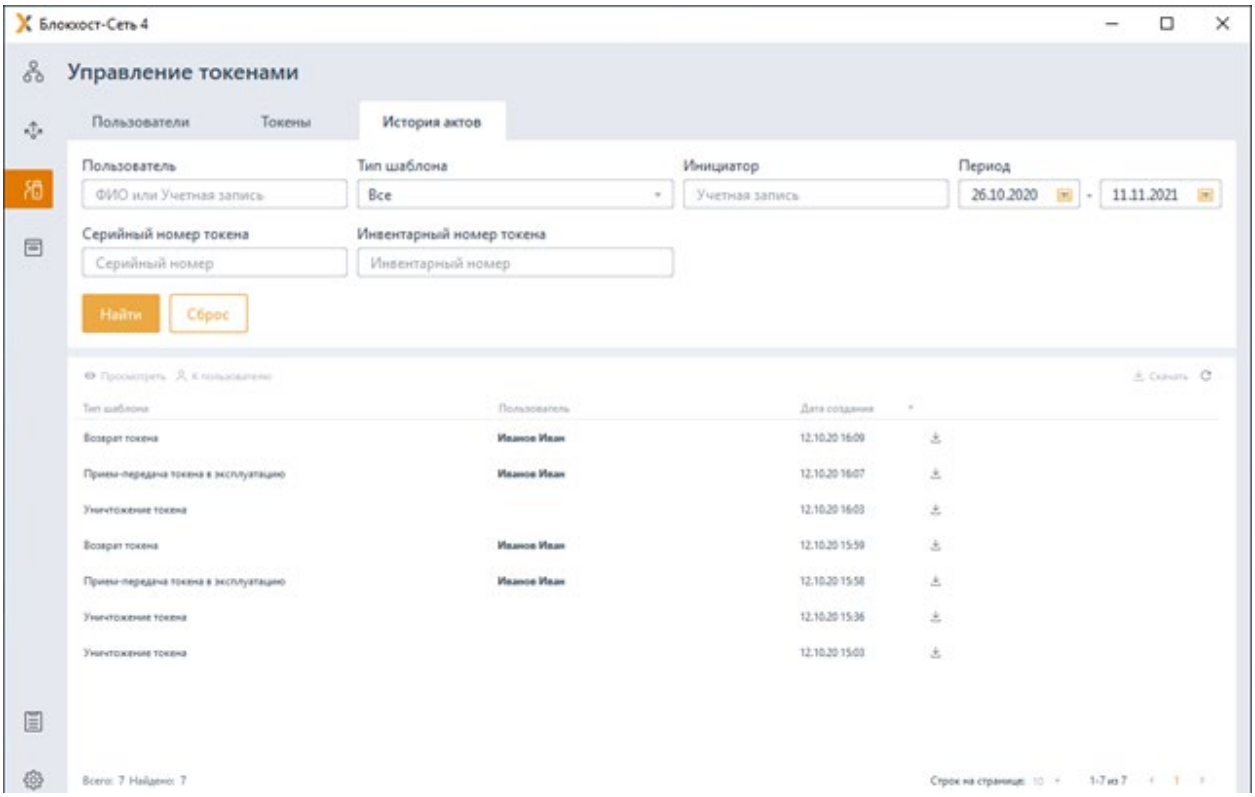


Рисунок 4.30 – Вкладка ***История актов***

Формирование актов возможно при выполнении ряда операций с токеном, перечисленных в таблице 4.3.

Таблица 4.3 – Типы актов в зависимости от выполняемой операции

Операция	Особенности выполнения	Тип акта
Выдача токена пользователю	с выпуском управляемого сертификата	«Запись сертификата на токен» «Прием-передача токена в эксплуатацию»
	с выпуском управляемого сертификата и удалением имеющегося на токене сертификата	«Запись сертификата на токен» «Удаление сертификата с токена» «Прием-передача токена в эксплуатацию»
	для безопасного входа по паролю	«Прием-передача токена в эксплуатацию»
	для учета	«Прием-передача токена в эксплуатацию»
	с выпуском стороннего сертификата	«Прием-передача токена в эксплуатацию»
Синхронизация токена	при отсутствии сертификата на токене (восстановление сертификата)	«Запись сертификата на токен»
	при истечении сертификата на токене (истекший сертификат удаляется, вместо него выпускается и записывается на токен актуальный сертификат для входа)	«Запись сертификата на токен» «Удаление сертификата с токена»
Изъятие токена		«Возврат токена»
Удаление токена из системы		«Уничтожение токена»

Для поиска нужного акта задайте один или несколько параметров поиска, расположенных в верхней части вкладки, и нажмите кнопку ***Найти***.

Возможен поиск по следующим параметрам:

– ***Пользователь*** – отображает список актов, сформированных при выпуске или изъятии токенов у заданного пользователя.

– ***Тип шаблона*** – поиск актов определенного типа.

– ***Инициатор*** – поиск актов по административной учетной записи, под которой выполняются операции с токеном (например, назначение токена пользователю).

– ***Период*** – поиск актов, сформированных за определенный промежуток времени.

– ***Серийный номер токена*** – поиск сформированных актов по заданному серийному номеру токена.

– ***Инвентарный номер токена*** – поиск сформированных актов по заданному инвентарному номеру токена.

Кнопка ***Сброс*** предназначена для очистки всех заданных ранее параметров поиска.

Проверить корректность сформированного акта возможно до выполнения сохранения акта на внешний носитель по кнопке 

.

Сохранить выбранный акт можно по кнопке  , в строке с найденным актом. При необходимости сохранения нескольких актов, выделите требуемые строки левой кнопкой мыши, удерживая клавишу ***Ctrl,*** или выделите диапазон строк, удерживая клавишу ***Shift***, и нажмите кнопку 

, расположенную в правом верхнем углу вкладки.

Необходимость формирования акта при определенной операции с токеном (операции, при которых возможно формирование актов, перечислены в таблице 4.3), возможность изменить шаблон акта или восстановить измененный шаблон на предустановленный в системе по умолчанию, осуществляется во вкладке ***Настройки*** в разделе ***«Шаблоны актов»*** (подробнее в разделе ***«Шаблоны актов»***).

5 Управление пользователями

Вкладка ***Пользователи*** предназначена для поиска пользователей и управления всеми устройствами (назначение, отзыв, синхронизация, включение и выключение) учетных записей пользователей, входящими в структуру Active Directory (рисунок 5.1).

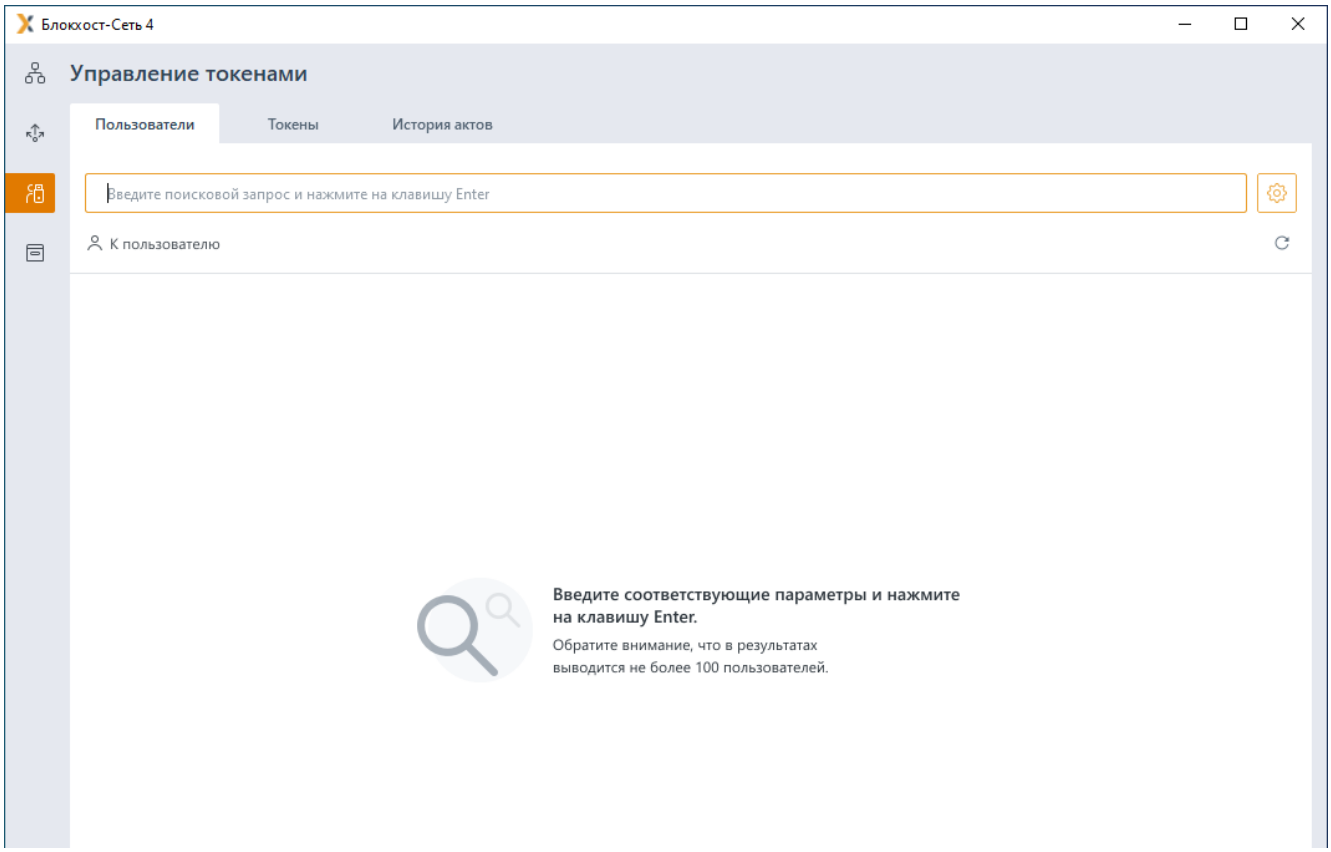


Рисунок 5.1 – Вкладка ***Пользователи***

5.1 Поиск пользователя

Для управления устройствами, привязанными к пользователю, необходимо найти нужного пользователя в подсистеме.

Для поиска пользователя перейдите на вкладку ***Пользователи***.

Введите в строке поиска часть символов или параметр целиком (рисунок 5.2), относящийся к учетной записи пользователя (наименование учетной записи, ФИО, телефон, почта).

Нажмите кнопку ***Найти***.

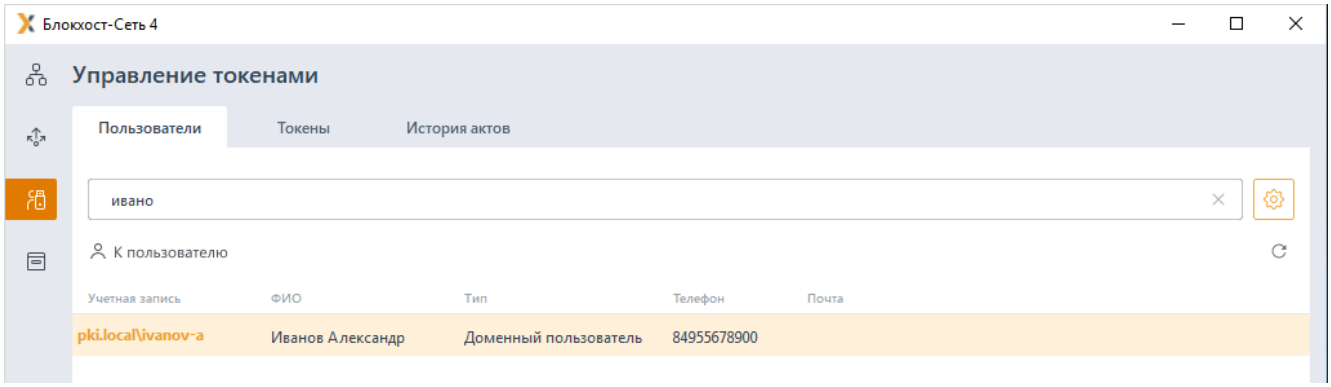


Рисунок 5.2 – Поиск пользователей

В списке отобразятся все пользователи, удовлетворяющие введенным символам любого параметра учетной записи.

Максимально возможное количество пользователей, отображаемых в списке – 100. При отсутствии необходимого пользователя в списке, укажите более точные параметры поиска.

5.2 Карточка пользователя

В карточке пользователя содержится информация о пользователе (ФИО пользователя, наименование учетной записи, телефон и электронная почта) и перечень назначенных устройств (рисунок 5.3).

Для перехода в профиль пользователя выполните поиск пользователя по известным параметрам во вкладке ***Пользователи***.

Перейдите в строку с пользователем, профиль которого необходимо просмотреть.

Нажмите на ссылку в столбце ***Учетная запись*** или перейдите по кнопке ***К пользователю***.

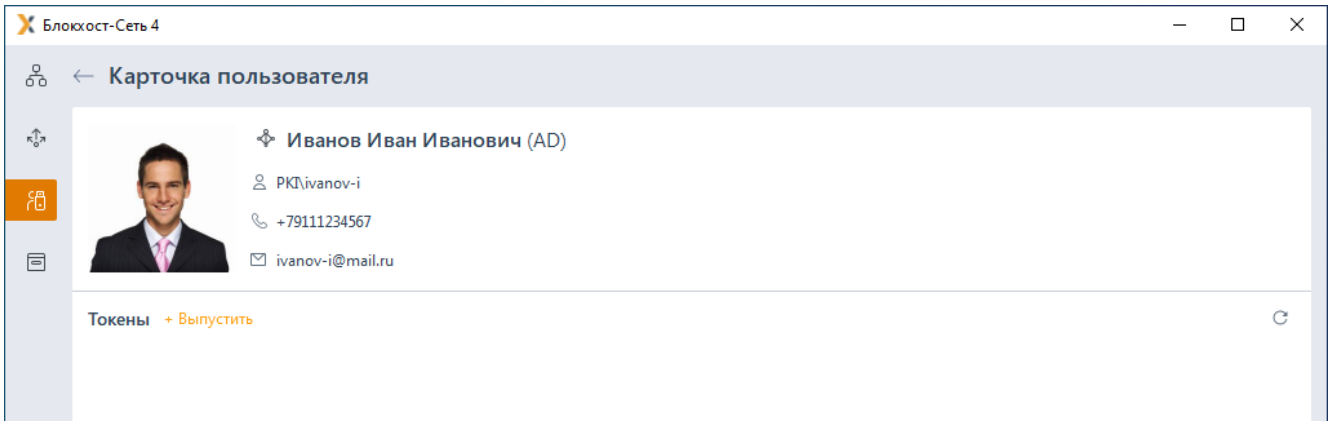


Рисунок 5.3 – Карточка пользователя

5.3 Назначение токена пользователю

Назначение токена пользователю заключается в привязке устройства конкретному пользователю.

Один токен может принадлежать только одному пользователю.
Пользователю может принадлежать несколько токенов.

Назначение устройства пользователю доступно во вкладках:

– ***Пользователи:***

- перейдите на вкладку ***Пользователи*** и выполните поиск пользователя;
- перейдите в профиль пользователя по ссылке в столбце ***Учетная запись***;
- нажмите ***Выпустить*** в области **Токены** (рисунок 5.4).

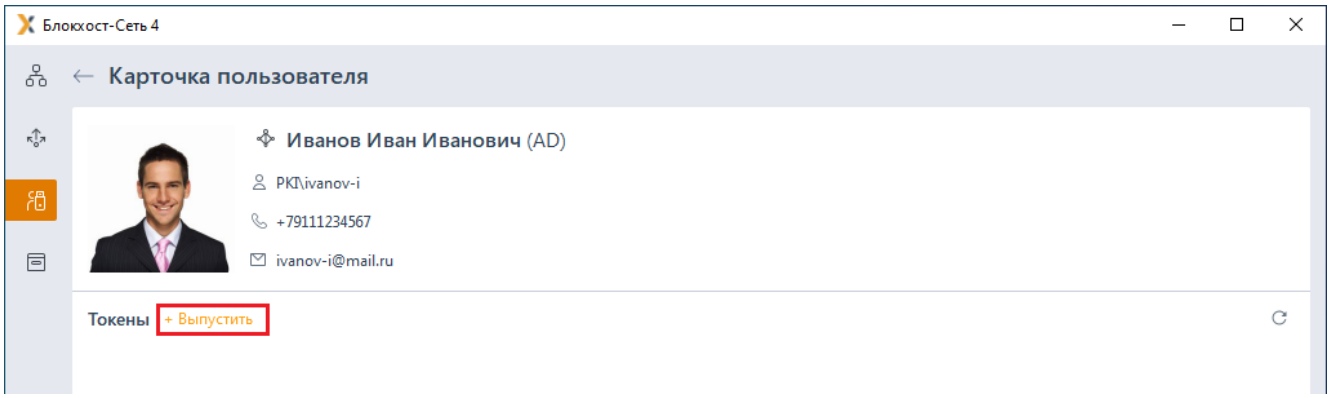


Рисунок 5.4 – Назначение токена пользователю

– ***Токены:***

- перейдите во вкладку ***Токены;***
- вызовите контекстное меню с помощью правой кнопки мыши;
- выберите ***Выпустить токен для*** (рисунок 5.5).

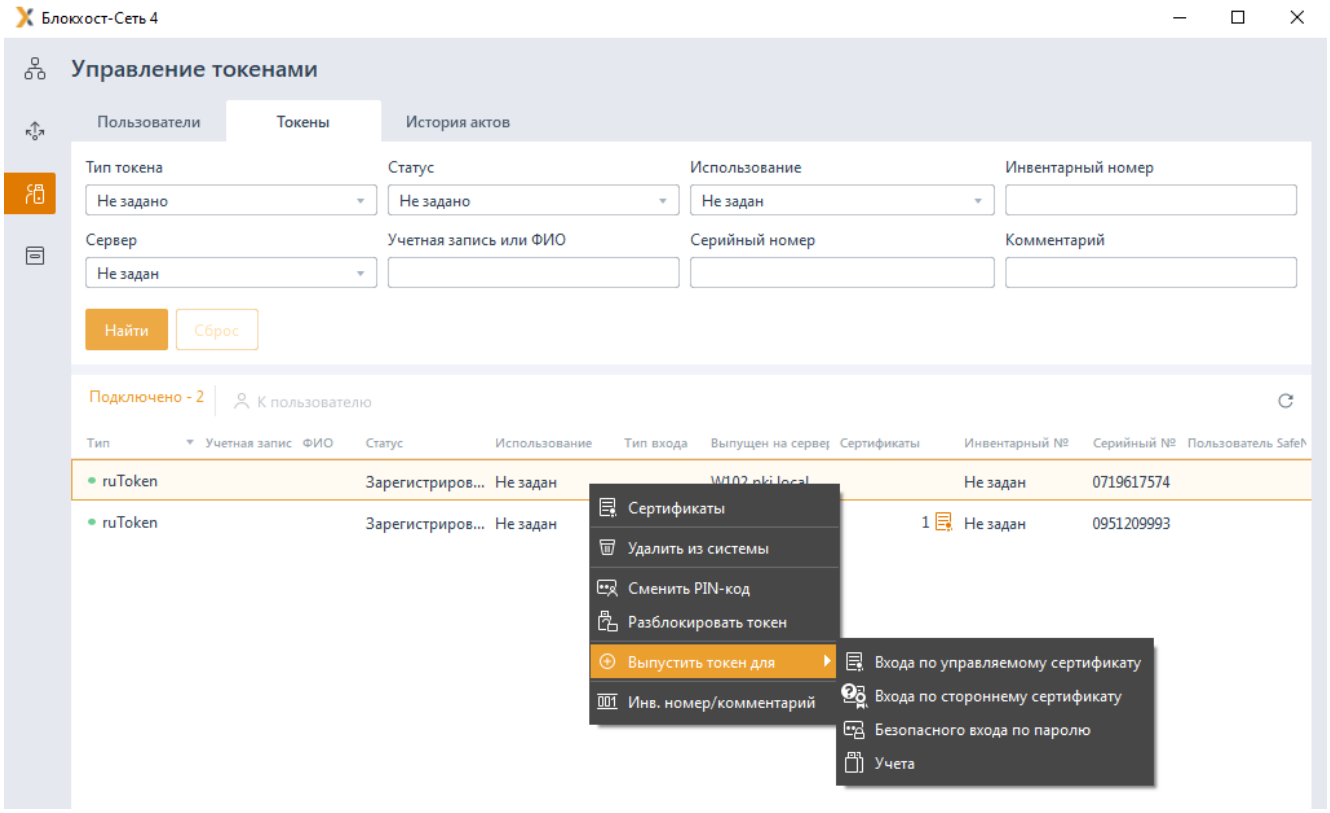


Рисунок 5.5 – Контекстное меню ***Выпустить***

– ***Подключенные токены:***

- перейдите во вкладку ***Токены***;
- перейдите по ссылке ***Подключено*** (рисунок 4.2);
- с помощью контекстного меню выберите ***Выпустить токен для…***.

Возможно назначение токена пользователю:

– для входа по управляемому сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный средствами подсистемы управления токенами);

– для входа по стороннему сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный сторонними средствами);

– для безопасного входа по паролю (при использовании токена для аутентификации по паролю, записанному на устройство);

– для учета.

5.3.1 Выпуск токена для учета

Токен без записи сертификата для входа назначается пользователю для учета в подсистеме жизненного цикла токенов и наблюдения, например, за сертификатами на токене, выданными сертифицированным удостоверяющим центром и используемыми для электронной подписи в юридическо-значимом документообороте.

Для присвоения токена пользователю для учета воспользуйтесь одним из способов, описанных в разделе **Назначение токена пользователю** (на рисунке 5.6 приведен пример назначения токена из карточки пользователя).

Нажмите ***Выпустить*** в области ***Токены*** и выберите ***Для учета*** (рисунок 5.6).

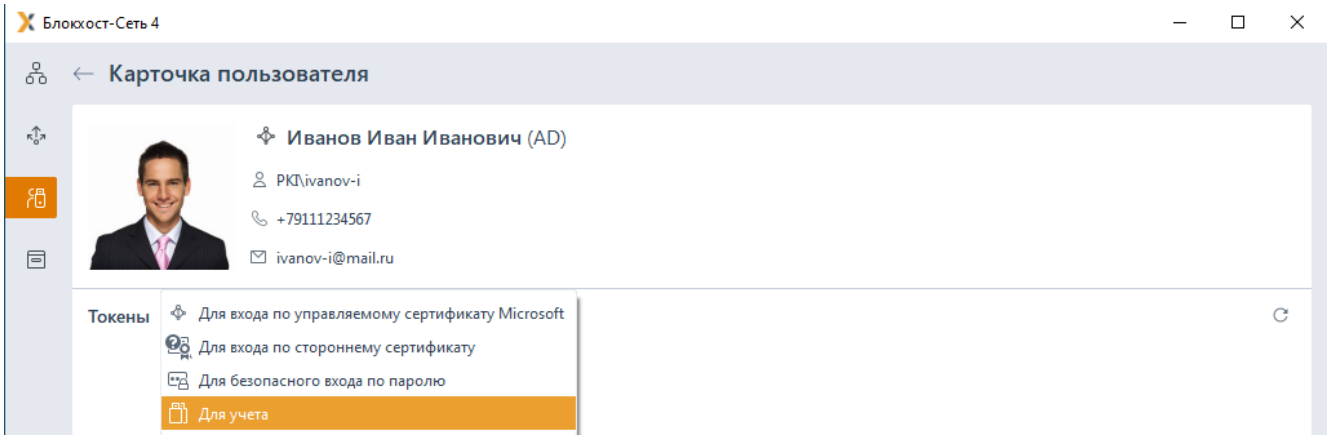


Рисунок 5.6 – Назначение токена для учета

Выберите из списка токен, который будет присвоен пользователю (рисунок 5.7), и нажмите ***Далее***.

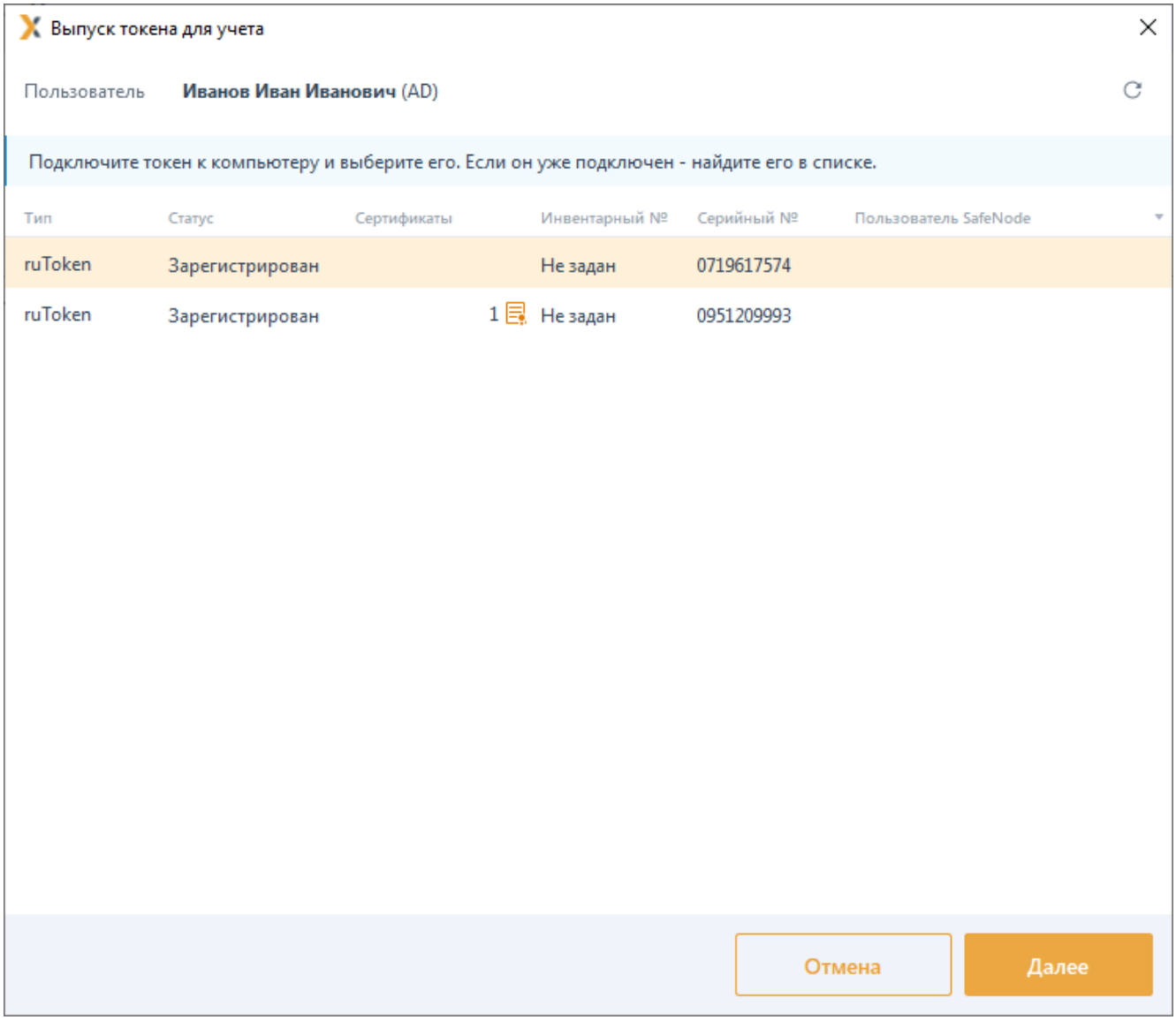


Рисунок 5.7 – Выбор токена для присвоения пользователю

Присваиваемый токен должен быть напрямую подключен к АРМ администратора, с установленной серверной версией СЗИ от НСД «Блокхост-Сеть 4».

Если токен не отображается в списке, проверьте правильность подключения токена и обновите список по кнопке «».

Введите инвентарный номер выдаваемого токена и, при необходимости, добавьте комментарий в следующем окне (рисунок 5.8).

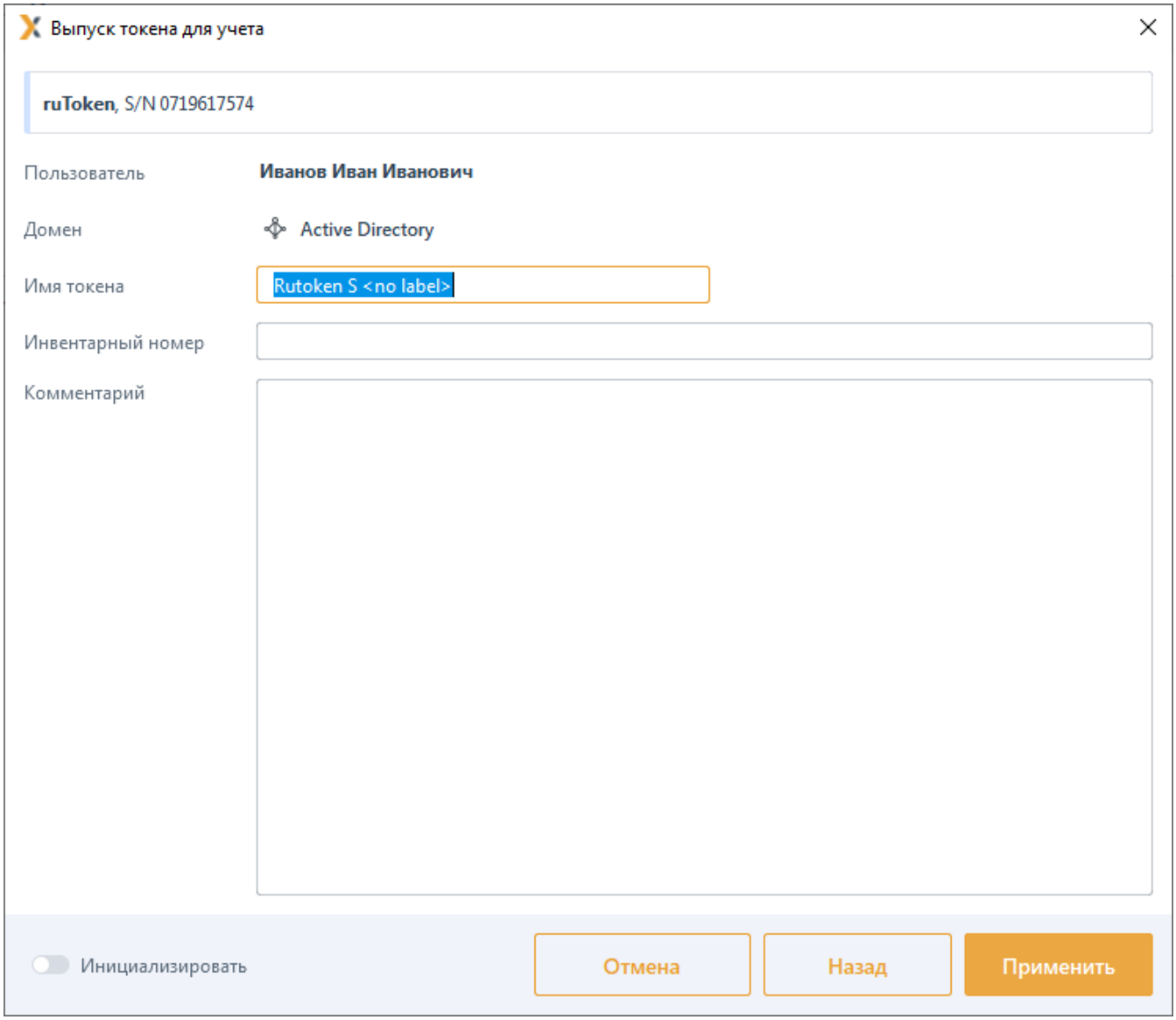


Рисунок 5.8 – Ввод параметров выдаваемого токена

При установке опции ***Инициализировать*** введите параметры инициализации в следующем окне и нажмите ***Применить***.

Установка параметров инициализации описана в разделе ***«Инициализация токена»***.

После успешного назначения токена без записи сертификата, необходимо нажать кнопку ***Закрыть*** (рисунок 5.9).

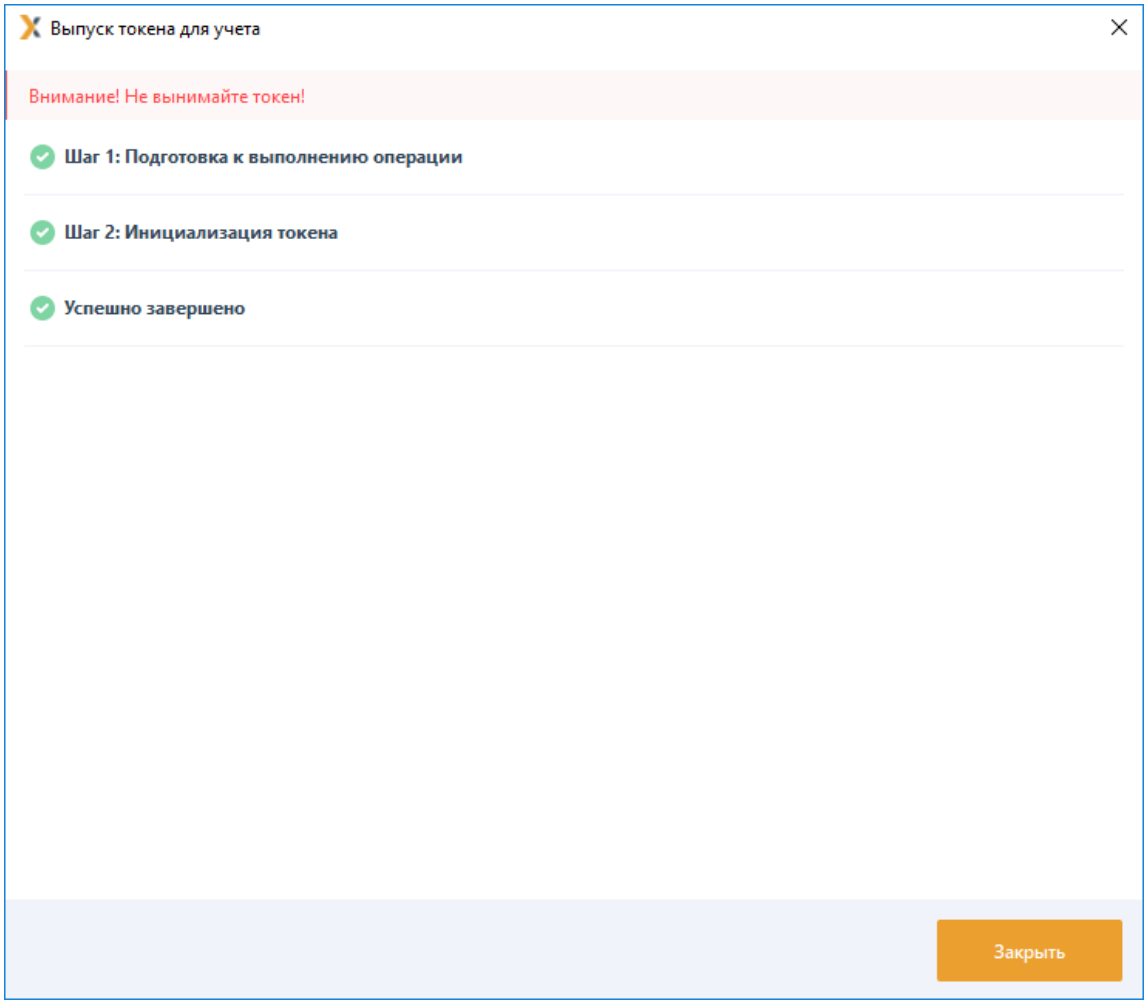


Рисунок 5.9 – Успешное назначение токена

В карточке пользователя, в области ***Токены*** появится устройство, назначенное пользователю (рисунок 5.10).

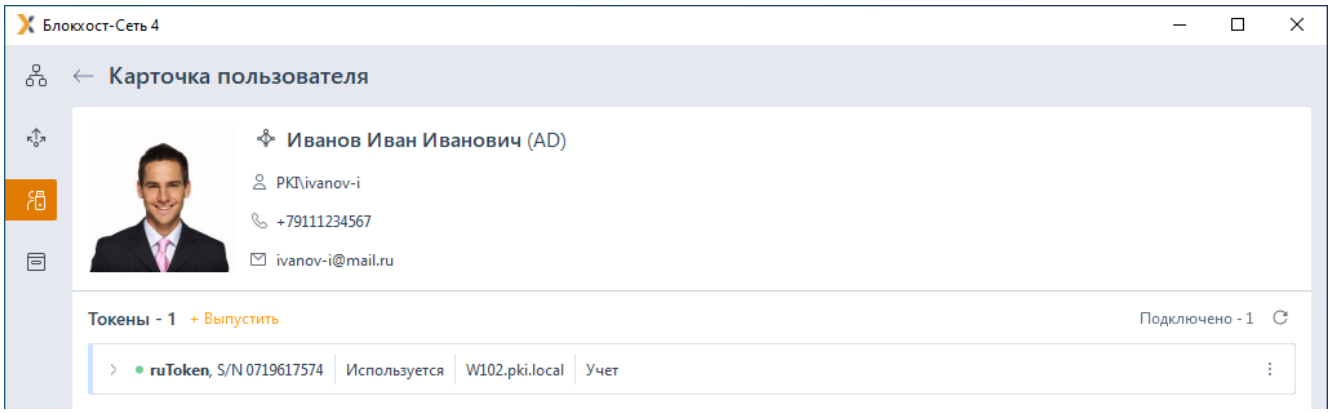


Рисунок 5.10 – Отображение токена для учета в карточке пользователя

5.3.2 Выпуск токена для безопасного входа по паролю

Назначение токена пользователя для аутентификации пользователя с использованием сложного сгенерированного пароля, хранимого на токене.

После назначения такого токена, пользователь может использовать токен со сгенерированным паролем для безопасного входа при аутентификации на своей рабочей станции при условии:

– наличия подключенного к АРМ пользователя токена;

– возможности аутентификации пользователя с использованием токена («Вход по токену») в политике аутентификации, назначенной пользователю/группе пользователей в которой он состоит.

Приглашение к переходу на аутентификацию с использованием токена для безопасного входа по паролю (БВПП) будет доступно пользователю после входа с использованием пароля, при выполнении описанных выше условий.

Аутентификация с использованием БВПП возможна:

1) По PIN-коду со сменой пароля.

Для перехода на аутентификацию с использованием токена с БВПП со сменой пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет изменен на сложную случайную последовательность, сгенерированную СЗИ и сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

Если во время перехода на аутентификацию с использованием БВПП не удалось изменить пароль пользователя (например, политика домена запрещает изменять пароль чаще чем 1 раз в день, а пароль уже был изменен), то на токен записывается текущий пароль пользователя, однако пользователю выводится предупреждение (рисунок 5.11).

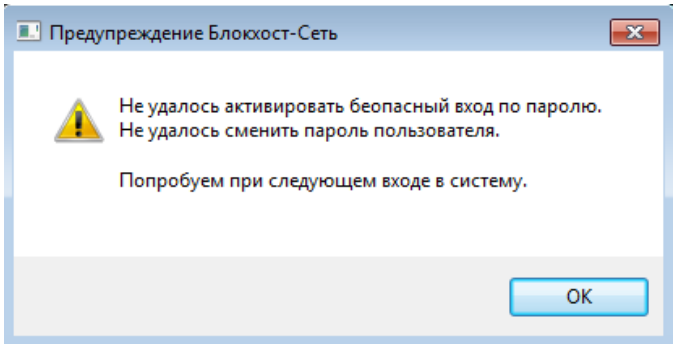


Рисунок 5.11 – Предупреждение при активации безопасного входа по паролю

При этом далее пользователь сможет входить с использованием токена, но попытка сменить пароль на сгенерированный будет производиться при каждом входе пользователя в систему, до момента пока он не будет изменен.

2) По PIN-коду без смены пароля.

Для перехода на аутентификацию с использованием токена с БВПП без смены пароля пользователю необходимо ввести PIN-код к ключевому носителю. После ввода PIN-кода, пароль пользователя будет сохранен на токен.

Последующий вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом PIN-кода токена вместо пароля. Пароль будет считан и предъявлен автоматически.

3) По паролю без PIN-кода.

Вход пользователя в ОС будет доступен только на клиентской рабочей станции с использованием назначенного токена и вводом пароля пользователя. PIN-код токена вводить не требуется.

Для присвоения токена пользователю для безопасного входа по паролю воспользуйтесь одним из способов, описанных в разделе ***«Назначение токена пользователю»*** (на рисунке 4.6 приведен пример назначения токена из карточки пользователя).

Нажмите ***Выпустить*** в области ***Токены*** и выберите ***Для безопасного входа по паролю*** (рисунок 5.12).

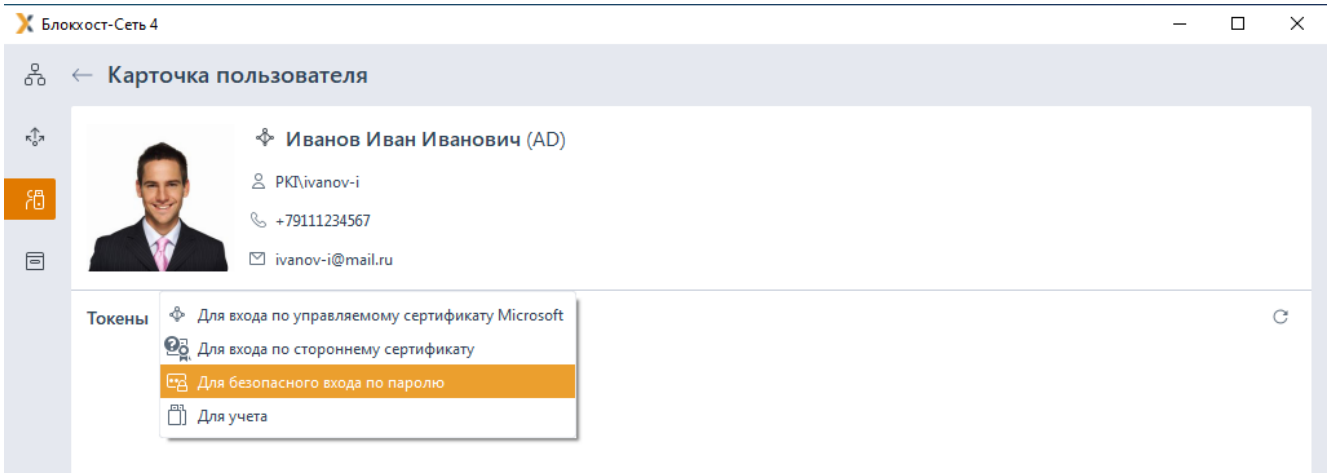


Рисунок 5.12 – Назначение токена для безопасного входа по паролю

Выберите из списка токен, который будет присвоен пользователю (рисунок 5.13), и нажмите ***Далее***.

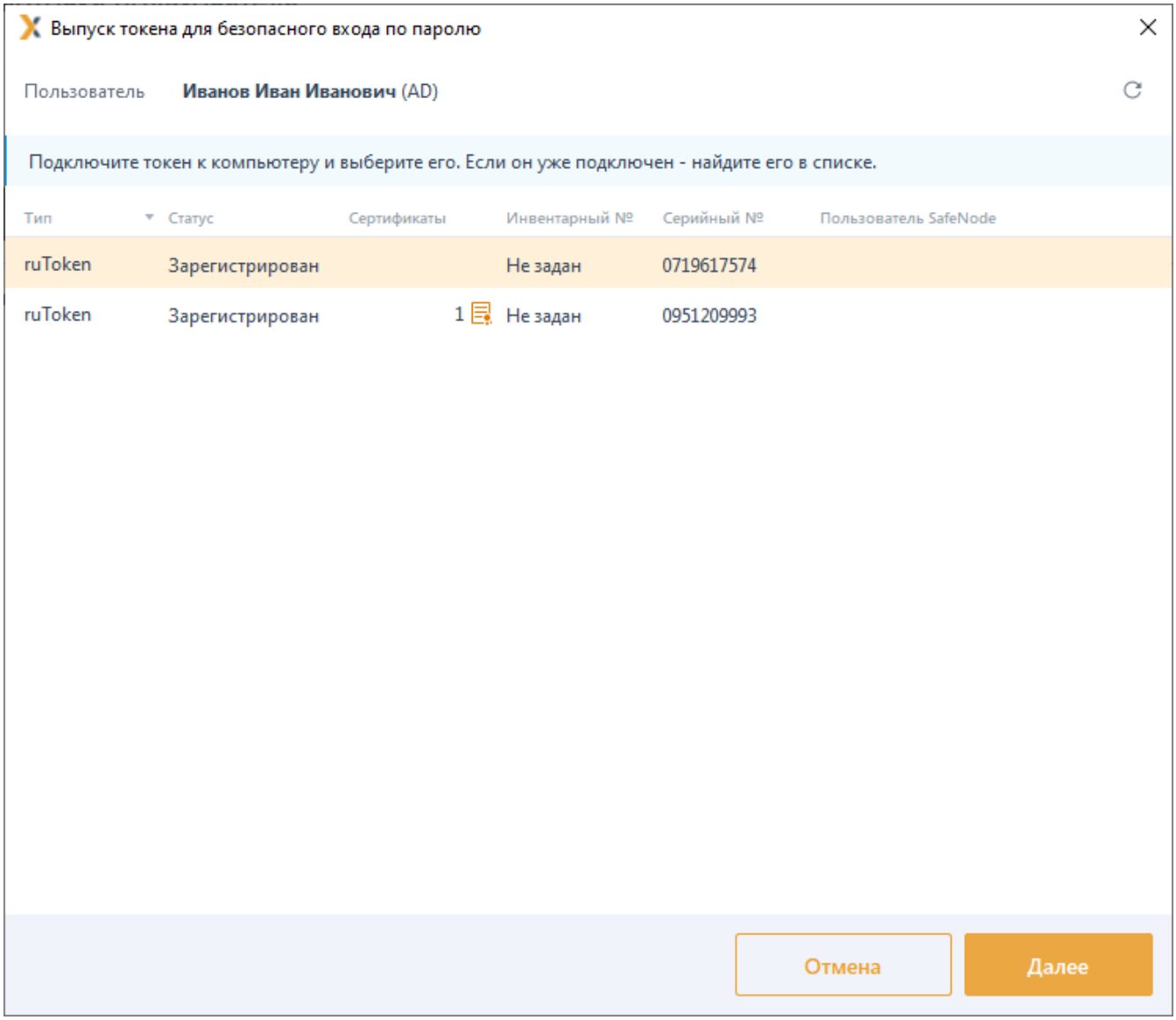


Рисунок 5.13 – Выбор токена для присвоения пользователю

Присваиваемый токен должен быть напрямую подключен к АРМ администратора, с установленной серверной версией СЗИ от НСД «Блокхост-Сеть 4».
Если токен не отображается в списке, проверьте правильность подключения токена и обновите список по кнопке «».

По кнопке ***Изменить*** (рисунок 5.15) выберите тип входа аутентификации с использованием БВПП (рисунок 5.14).

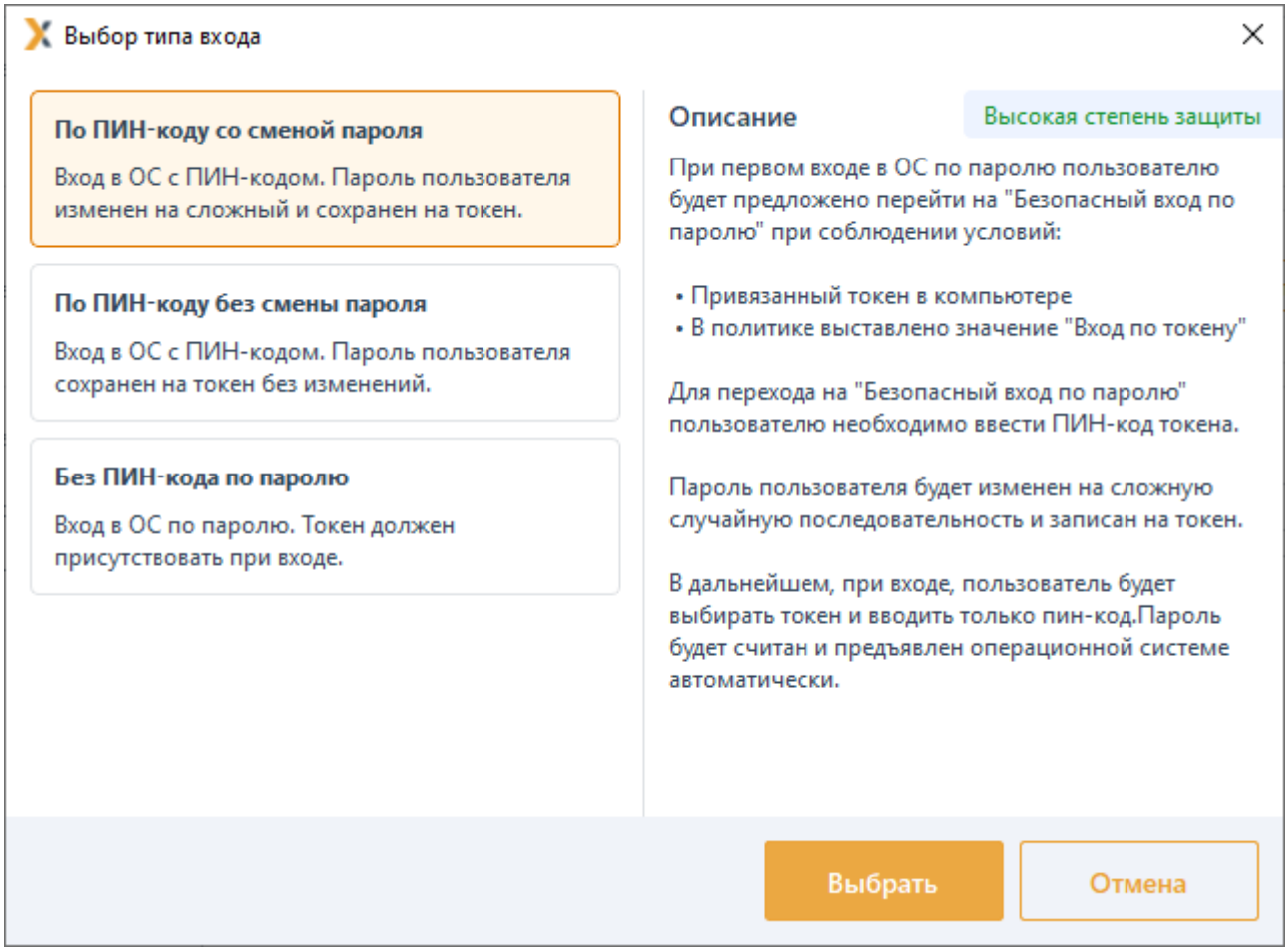


Рисунок 5.14 – Выбор типа входа БВПП

Введите инвентарный номер выдаваемого токена и, при необходимости, добавьте комментарий в соответствующем поле (рисунок 5.15).

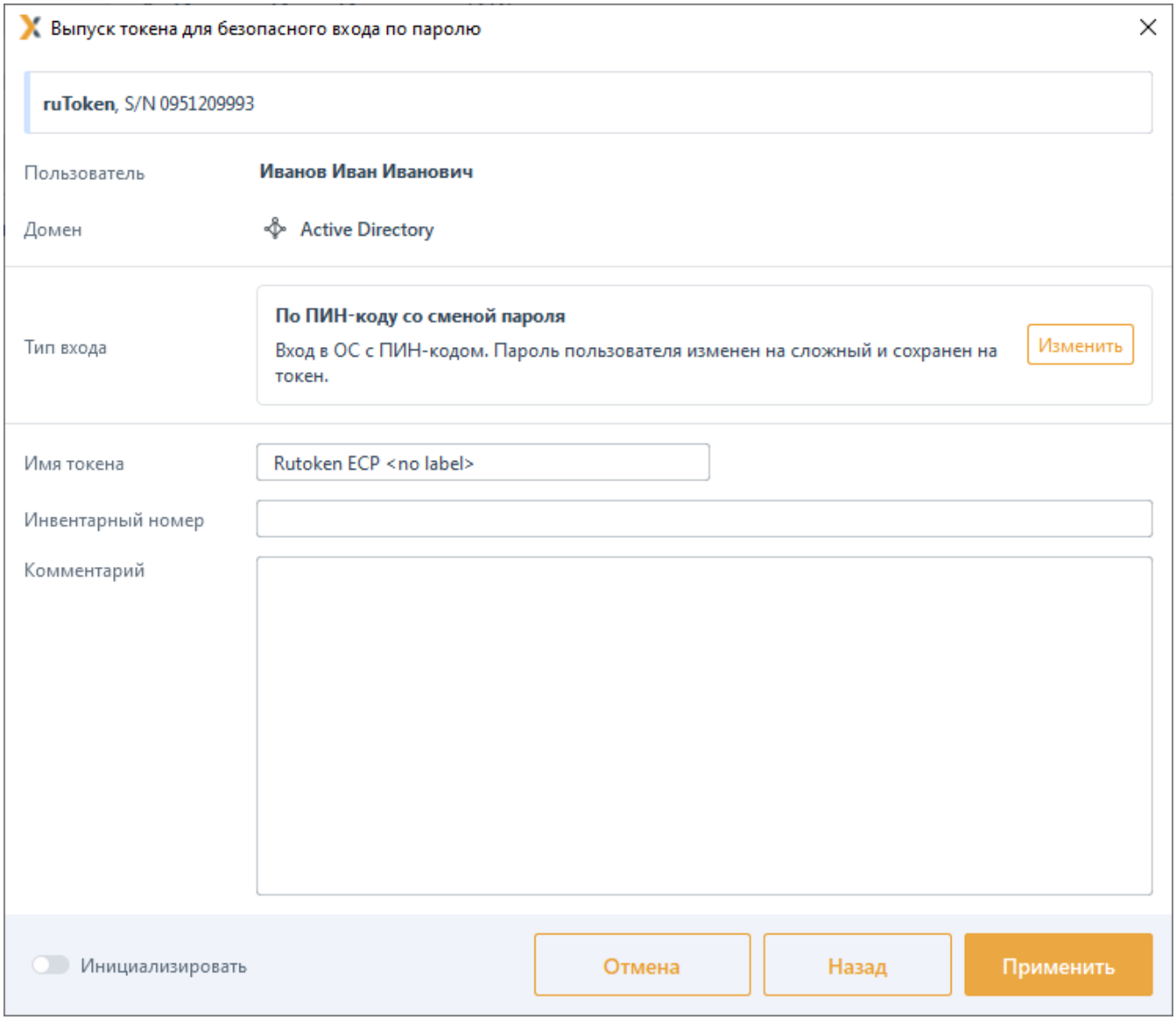


Рисунок 5.15 – Ввод параметров выдаваемого токена

При установке опции ***Инициализировать*** введите параметры инициализации в следующем окне и нажмите ***Применить***.

Установка параметров инициализации описана в разделе ***«Инициализация токена»***.

После успешного назначения токена для безопасного входа по паролю, в карточке пользователя, в области ***Токены*** появится устройство, назначенное пользователю (рисунок 5.16).

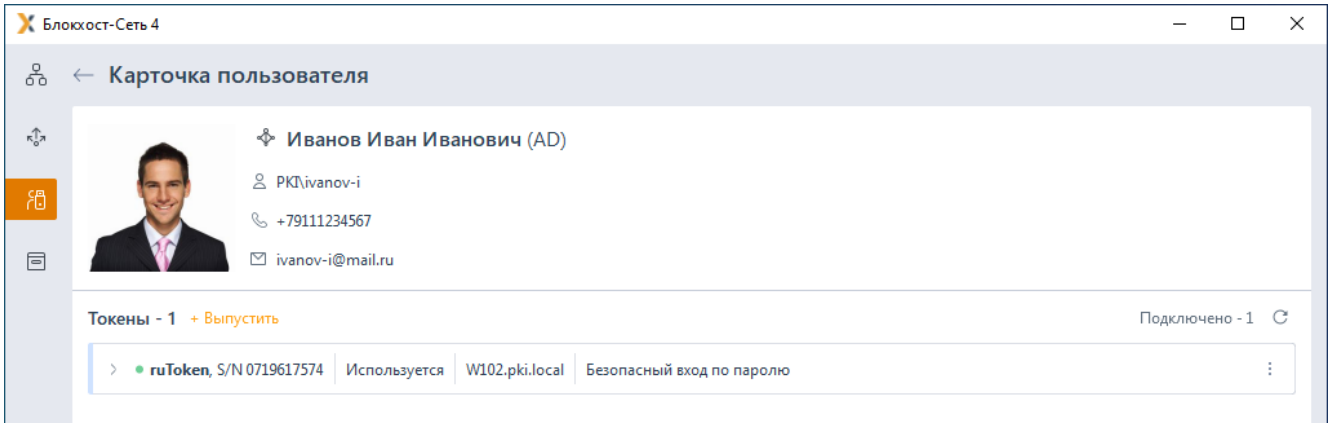


Рисунок 5.16 – Отображение токена для входа по паролю в карточке пользователя

5.3.3 Выпуск токена для входа по управляемому сертификату

Назначение токена пользователю для аутентификации с использованием цифрового сертификата, выпущенному средствами подсистемы управления токенами.

Для присвоения токена пользователю для входа по управляемому сертификату воспользуйтесь одним из способов, описанных в разделе ***«Назначение токена пользователю»*** (на рисунке 5.17 приведен пример назначения токена из карточки пользователя).

Нажмите ***Выпустить*** в области ***Токены*** и выберите ***Для входа по управляемому сертификату*** (рисунок 5.17).

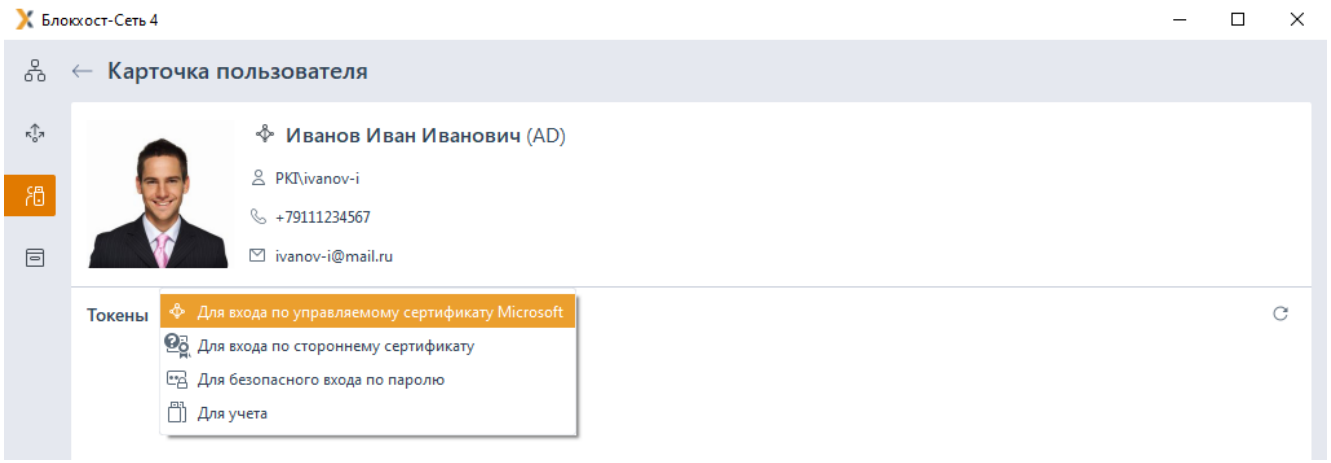


Рисунок 5.17 – Назначение токена для входа по управляемому сертификату

При возникновении ошибки вида, изображенного на рисунок 5.18, настройте выпуск сертификатов в соответствии с документами «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA», «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag».

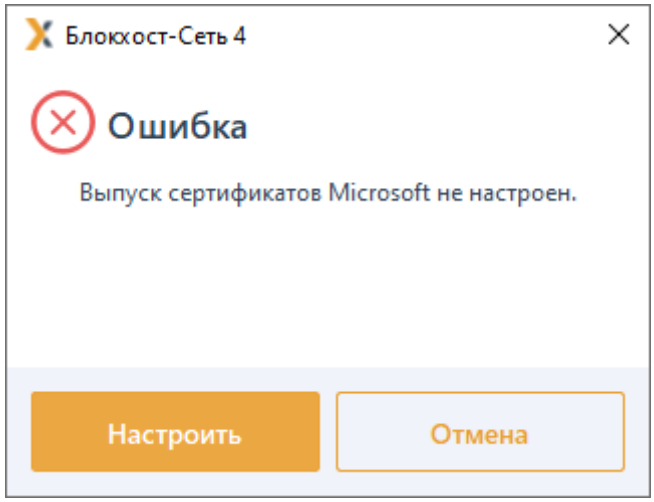
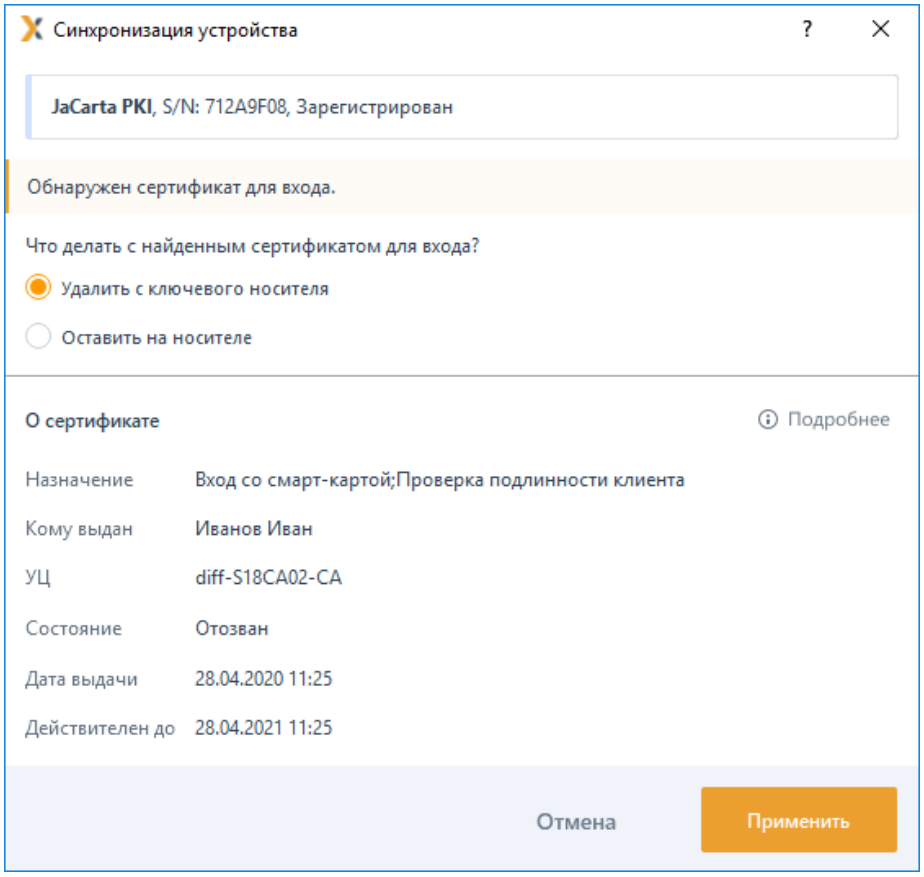


Рисунок 5.18 – Выпуск сертификатов не настроен

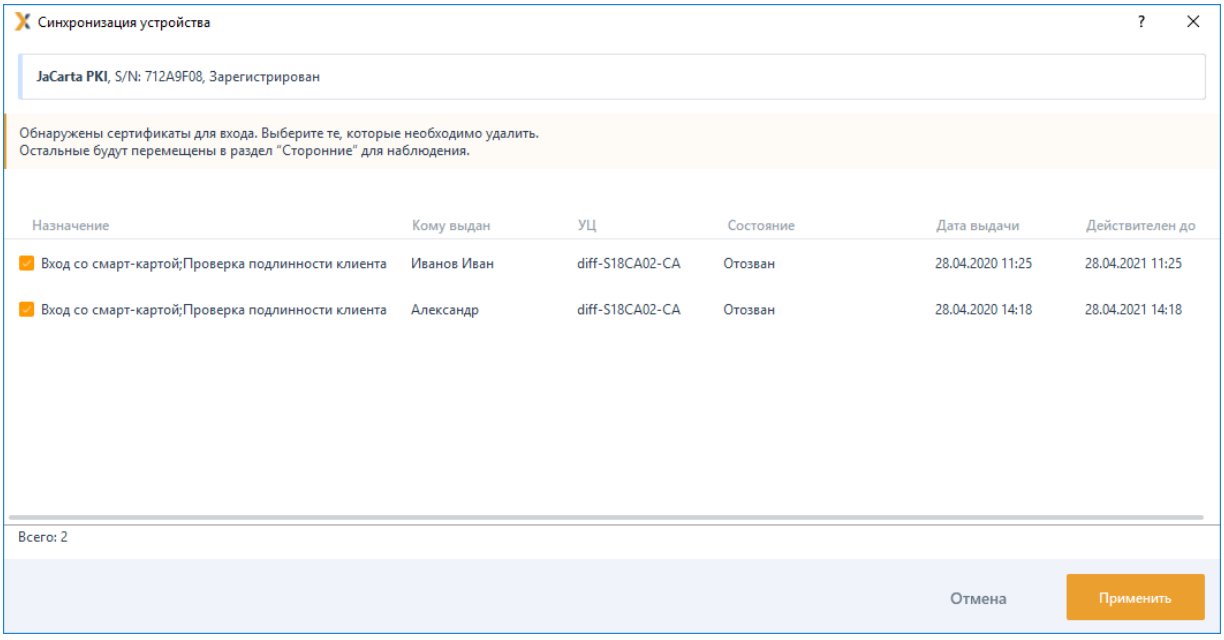
Выберите из списка токен, который будет присвоен пользователю (рисунок 5.7), и нажмите ***Далее***.

Присваиваемый токен должен быть напрямую подключен к АРМ администратора, с установленной серверной версией СЗИ от НСД «Блокхост-Сеть 4».
Если токен не отображается в списке, проверьте правильность подключения токена и обновите список по кнопке «».

Если на токене, назначаемом пользователю, уже есть сертификаты для входа (имеют признак «Вход по смарт-карте»), при этом не проводится инициализация назначаемого токена, появится окно для выбора действий с такими сертификатами: удалить или перенести в список сертификатов для наблюдения (рисунок 5.19 а, б).



а)



б)

Рисунок 5.19 – Ошибка при назначении токена с записью управляемого сертификата

Выберите профиль для выпуска токена, ведите имя токена, инвентарный номер выдаваемого токена и, при необходимости, добавьте комментарий в следующем окне (рисунок 5.20).

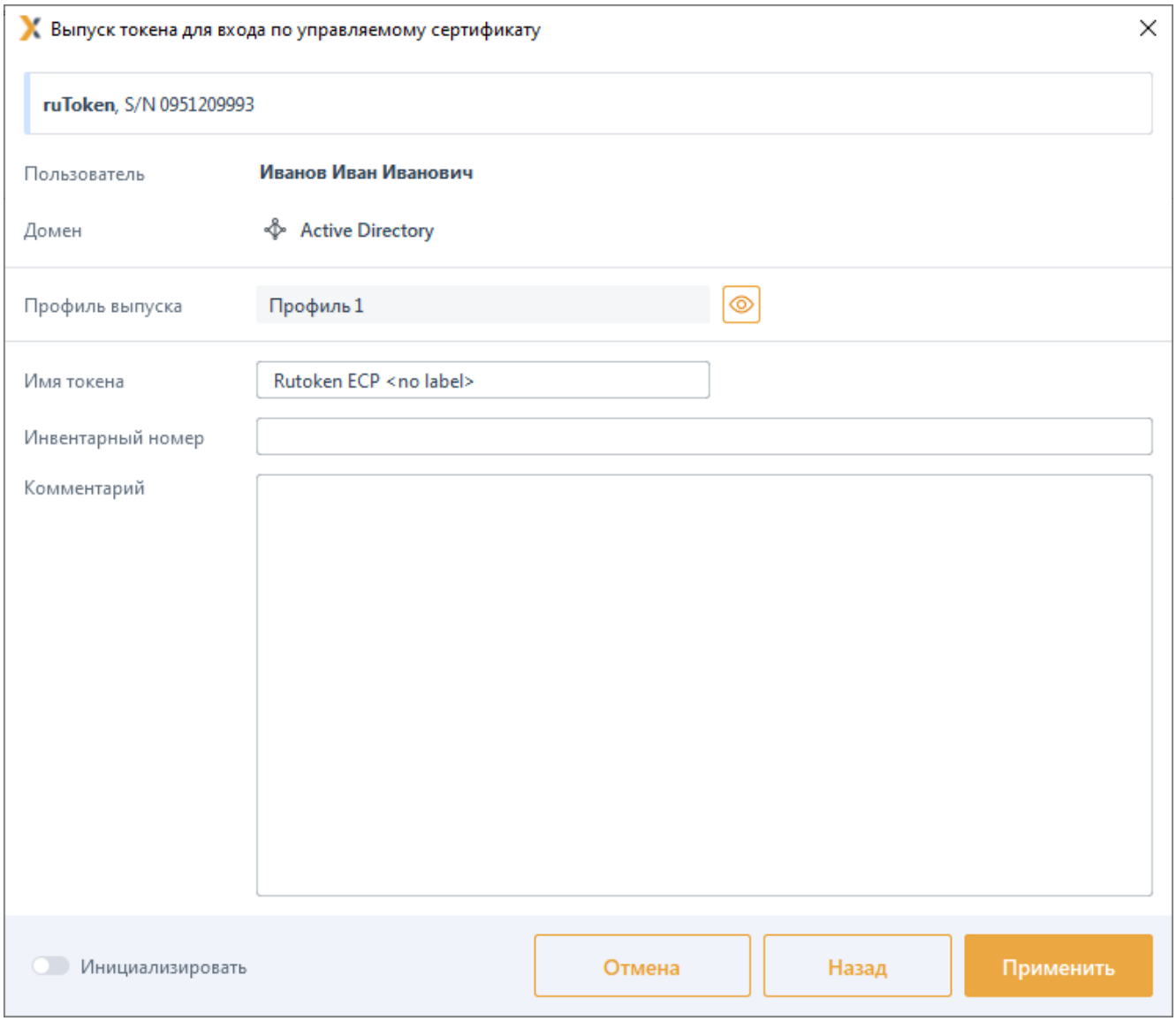


Рисунок 5.20 – Ввод данных для выпуска токена

При установке опции ***Инициализировать*** введите параметры инициализации в следующем окне и нажмите ***Применить***.

Установка параметров инициализации описана в разделе ***«Инициализация токена»***.

После нажатия кнопки ***Применить***, появится окно, отражающее процесс создания цифрового сертификата и записи сертификата на токен (рисунок 5.21).

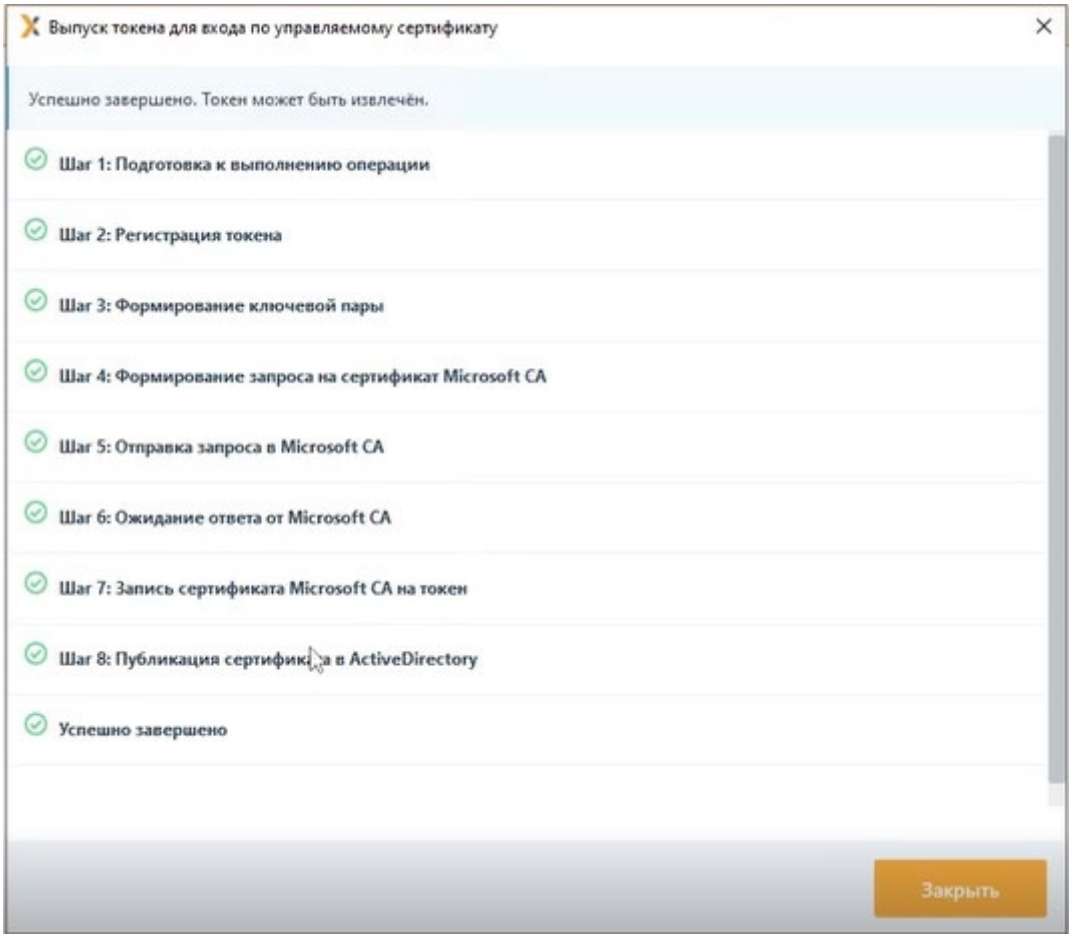


Рисунок 5.21 – Создание и запись сертификата на токен

До окончания записи сертификата на токен устройство вынимать **запрещено!**

Опция смены PIN-кода при первом входе пользователя в ОС установлена по умолчанию (рисунок 5.21) и осуществляется средствами СЗИ при входе пользователя с помощью этого сертификата.

После успешного завершения назначения пользователю токена для входа по управляемому сертификату, необходимо нажать кнопку ***Закрыть***.

В карточке пользователя, в области ***Токены,*** появится присвоенный пользователю токен с записанным цифровым сертификатом (рисунок 5.22).

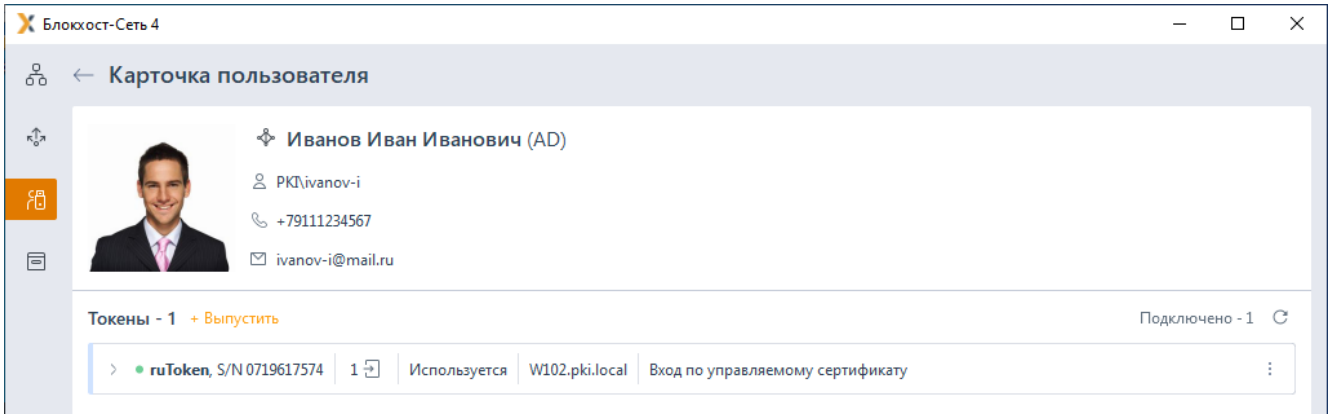


Рисунок 5.22 – Отображение токена для входа по управляемому сертификату в карточке пользователя

5.3.4 Выпуск токена для входа по стороннему сертификату

Токен для входа по стороннему сертификату назначается пользователю для аутентификации с использованием цифрового сертификата, выпущенному сторонними средствами.

Для присвоения токена пользователю для входа по стороннему сертификату воспользуйтесь одним из способов, описанных в разделе **Назначение токена пользователю** (на рисунке 5.23 приведен пример назначения токена из карточки пользователя).

Нажмите ***Выпустить*** в области ***Токены*** и выберите ***Для входа по стороннему сертификату*** (рисунок 5.23).

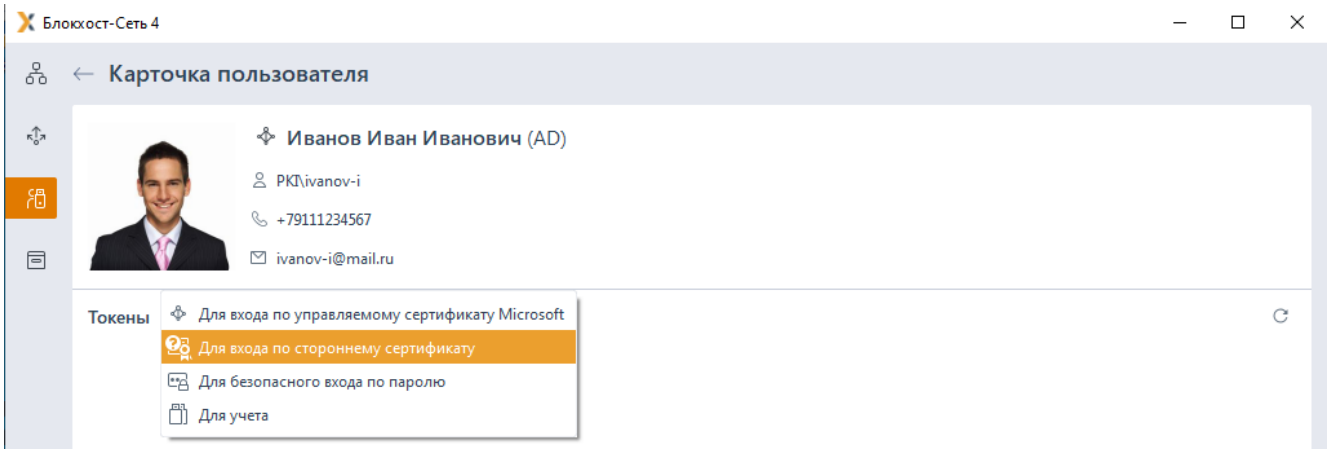


Рисунок 5.23 – Назначение токена для входа по стороннему сертификату

Дальнейшие действия по назначению токена пользователю аналогичны выпуску токена пользователю для учета и описаны в разделе ***«Выпуск токена для учета»***.

В окне на рисунке 5.24, отражающем процесс успешного назначения пользователю токена для входа по стороннему сертификату, необходимо нажать кнопку ***Закрыть***.

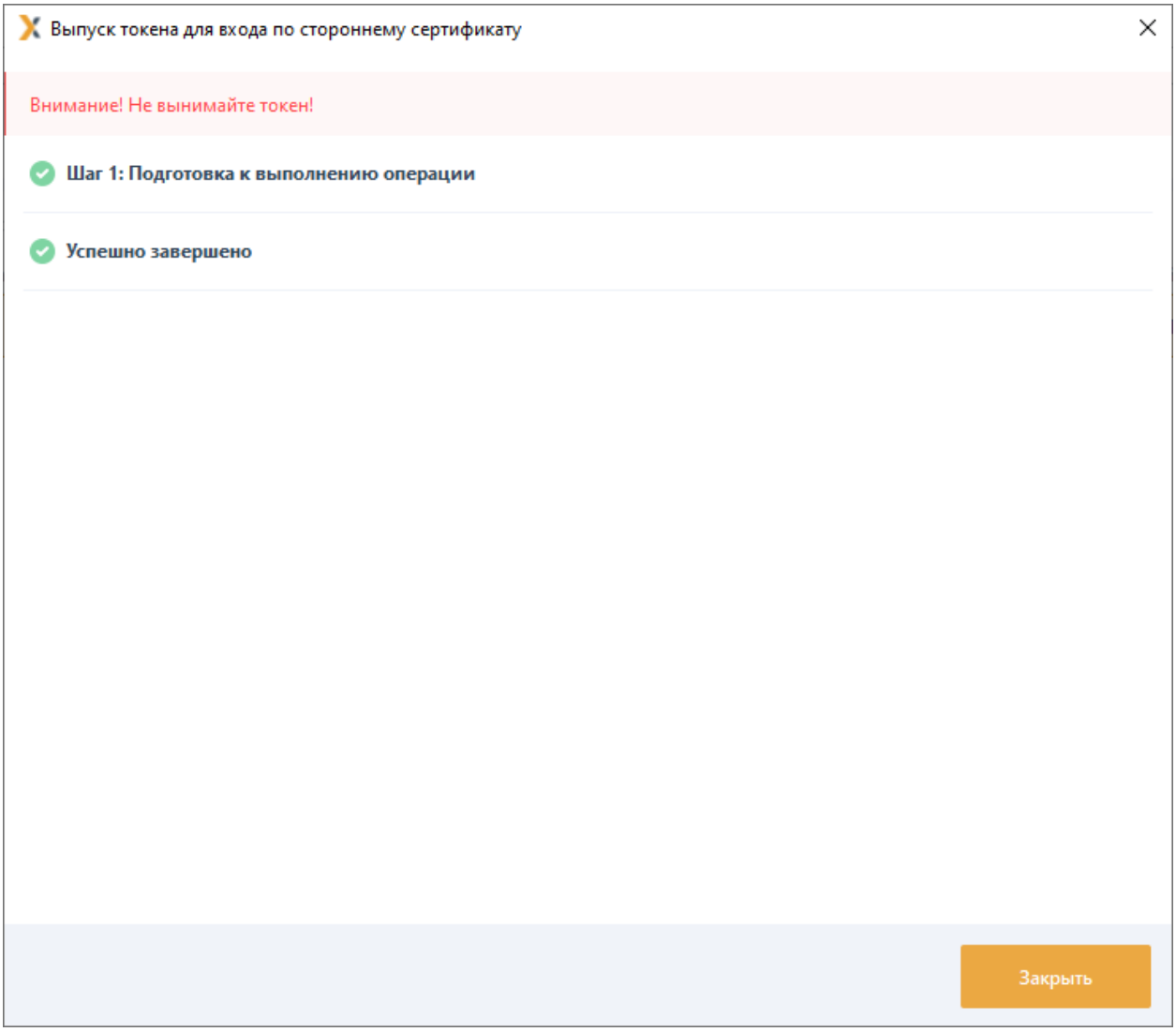


Рисунок 5.24 – Успешное назначение токена для входа по стороннему сертификату

В карточке пользователя, в области ***Токены*** появится устройство, назначенное пользователю (рисунок 5.25).

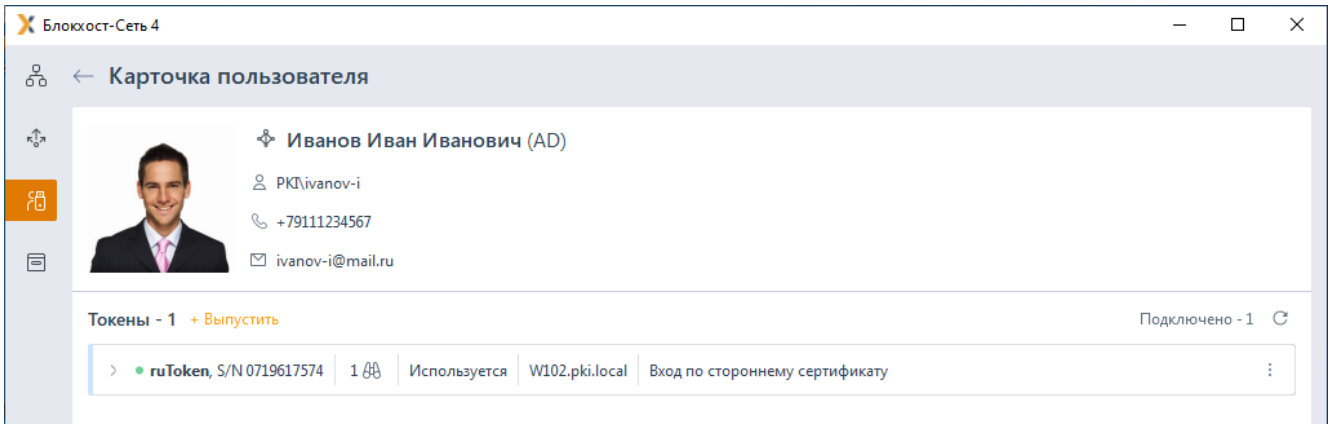


Рисунок 5.25 – Отображение токена для входа по стороннему сертификату в карточке пользователя

5.4 Привязка пользователя SafeNode

При управлении СЗИ от НСД «Блокхост-Сеть 4» средством доверенной загрузки «SafeNode System Loader», которое позволяет установить дополнительный этап прохождения аутентификации пользователей до загрузки ОС, существует возможность привязывать локального пользователя SafeNode к существующей связке токен ↔ пользователь.

Привязать пользователя SafeNode можно только к токену, назначенному пользователю для входа по БВПП, входа по управляемому сертификату или входа по стороннему сертификату.

Привязка пользователя SafeNode к существующей связке токен ↔ пользователь доступна во вкладках:

– ***Пользователи:***

- перейдите на вкладку ***Пользователи*** и выполните поиск пользователя;
- перейдите в профиль пользователя по ссылке в столбце ***Учетная запись***;
- вызовите контекстное меню с помощью нажатия правой кнопки мыши на токене пользователя, выпущенному для входа по БВПП, по управляемому сертификату или по стороннему сертификату, и выберите ***Привязать пользователя SafeNode*** (рисунок 5.26).

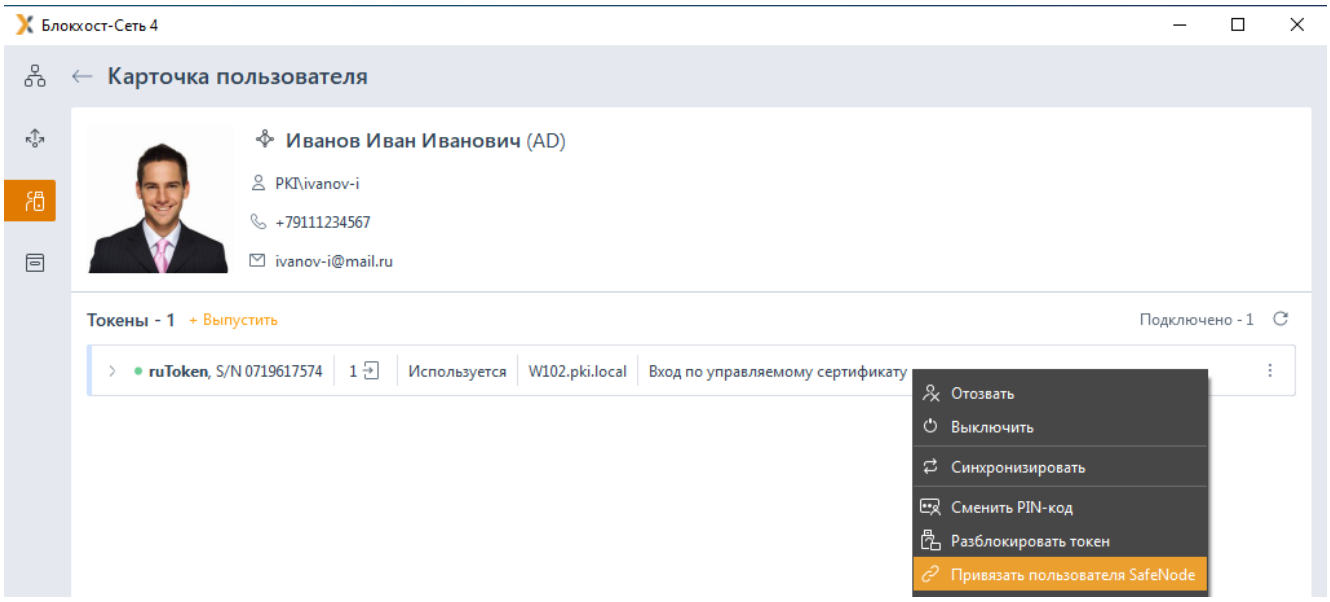


Рисунок 5.26 – Контекстное меню ***Привязать пользователя SafeNode***

– ***Токены:***

- перейдите во вкладку ***Токены;***
- выберите токен, выпущенный для входа по БВПП, по управляемому

сертификату или по стороннему сертификату;

- вызовите контекстное меню с помощью нажатия правой кнопки мыши и выберите ***Привязать пользователя SafeNode*** (рисунок 5.27).

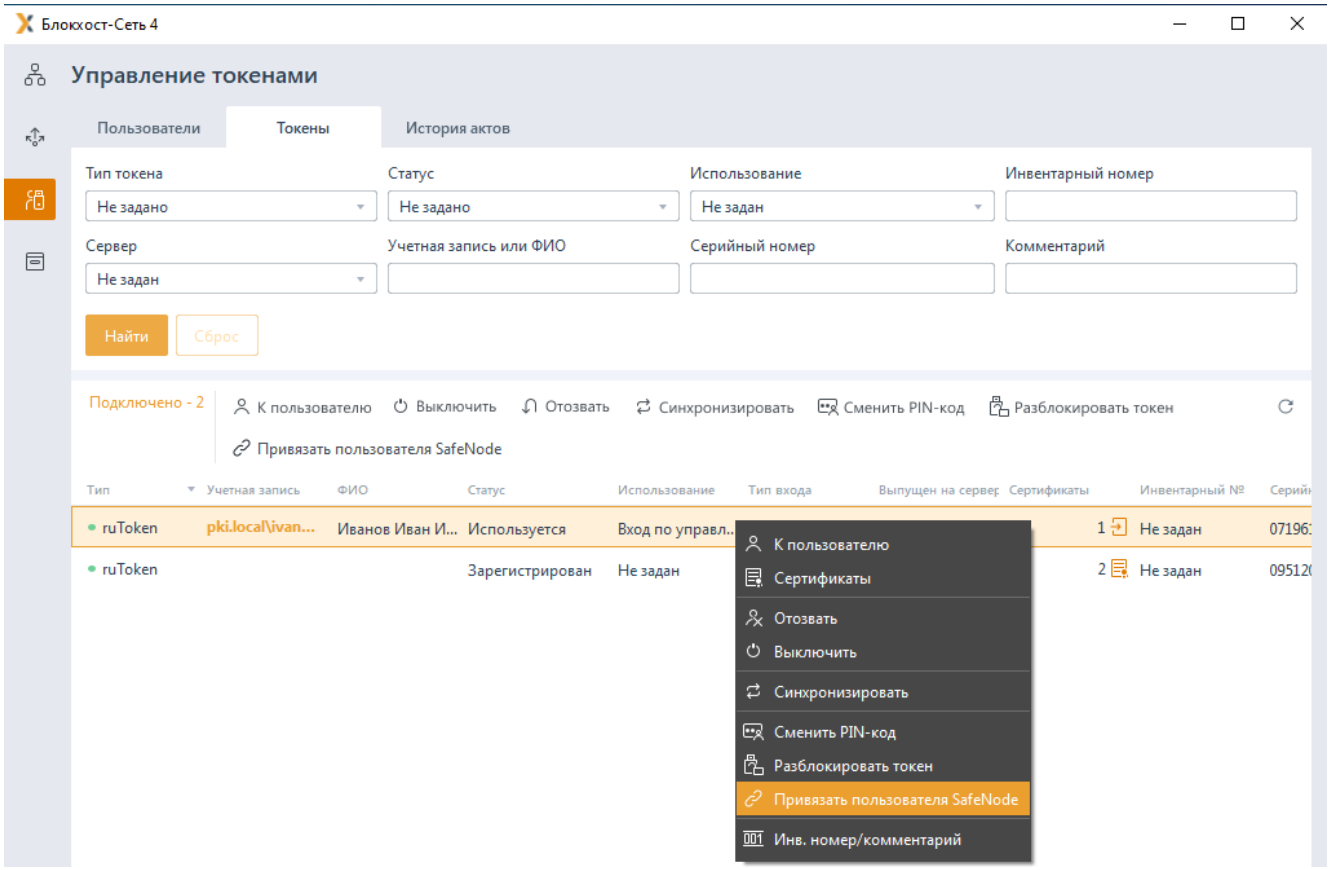


Рисунок 5.27 – Привязка пользователя SafeNode

– ***Подключенные токены:***

- перейдите во вкладку ***Токены***;
- перейдите по ссылке ***Подключено*** (рисунок 4.2);
- выберите токен, выпущенный для входа по БВПП, по управляемому сертификату или по стороннему сертификату;
- вызовите контекстное меню с помощью нажатия правой кнопки мыши и выберите ***Привязать пользователя SafeNode***.

После выбора пункта контекстного меню ***Привязать пользователя SafeNode*** появится окно, содержащее рабочие станции с установленным и взятым под управление СДЗ «SafeNode System Loader» (рисунок 5.28).

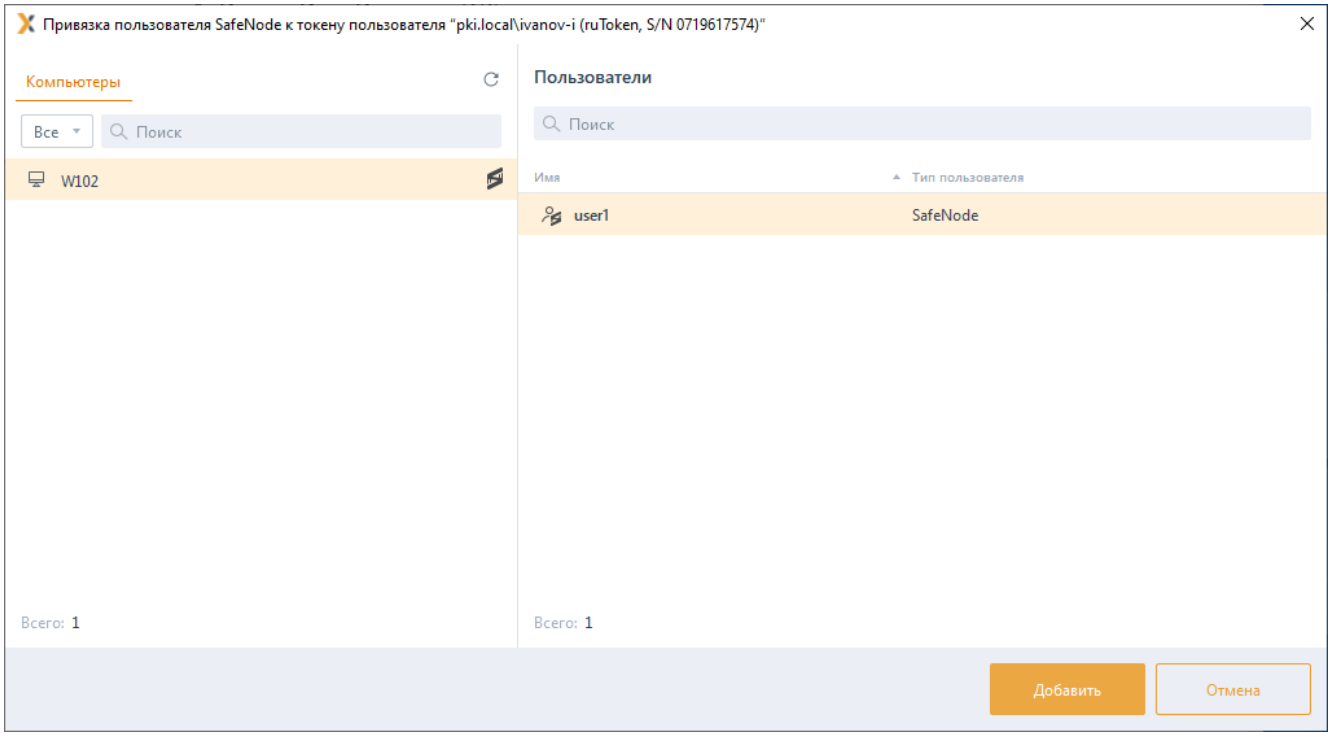


Рисунок 5.28 – Выбор пользователя SafeNode для привязки

При добавлении пользователей SafeNode, если на выбранной рабочей станции не установлено или не взято под управление СДЗ «SafeNode System Loader», выбор пользователей будет недоступен.

Выберите пользователя SafeNode, которого необходимо привязать к существующей связке токен ↔ пользователь и нажмите ***Добавить***.

Появится сообщение об успешной привязке пользователя SafeNode и добавленный пользователь отобразится в строке токена в поле ***Пользователь SafeNode*** (рисунок 5.29).

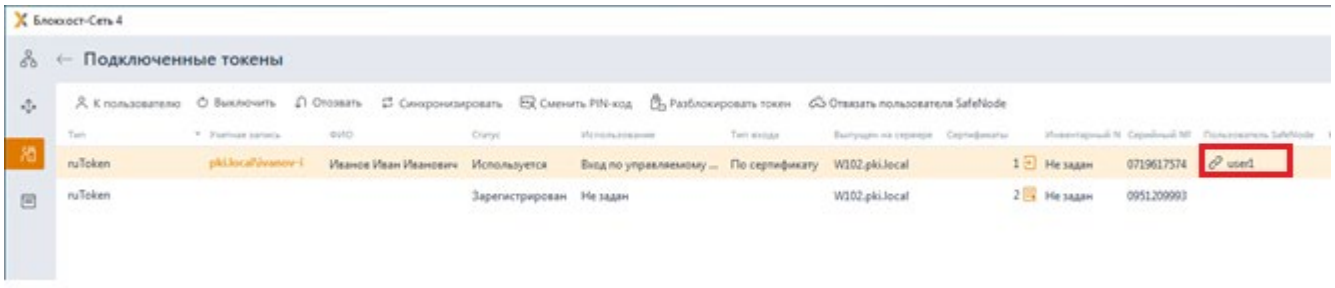


Рисунок 5.29 – Отображение добавленного пользователя SafeNode

Для того, чтобы удалить добавленного пользователя SafeNode из связки токен ↔ пользователь вызовите контекстное меню с помощью нажатия правой кнопки мыши и выберите ***Отвязать пользователя SafeNode***. При этом пользователь SafeNode будет отвязан без отзыва токена.

5.5 Удаленное назначение токена пользователю

Удаленное управление токенами осуществляется во вкладке ***Менеджер иерархии*** доступной по кнопке  (рисунок 5.30).

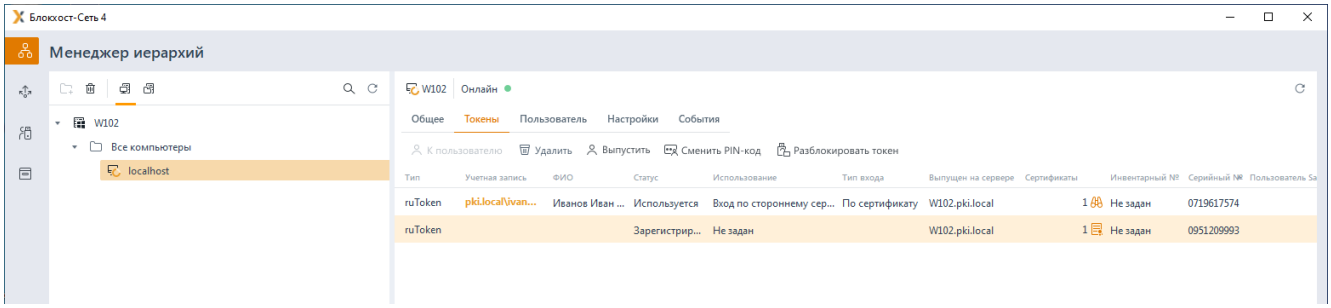


Рисунок 5.30 – Переход к рабочей станции в иерархии

Удаленное управление токенами доступно только при переходе в дереве иерархии на рабочую станцию, на которой необходимо осуществить привязку *токен ↔ пользователь*, во вкладках ***Токены/Пользователь***:

– во вкладке ***Токены*** отображается список токенов, подключенных к выбранной в иерархии рабочей станции (рисунок 5.30).

Для корректного отображения вошедшего доменного пользователя на удаленном компьютере в ОС Linux необходимо, отредактировать файл ***/etc/sssd/sssd.conf*** командой:

```
sudo pluma /etc/sssd/sssd.conf
```

и добавить строки:

```
case_sensitive = Preserving
use_fully_qualified_names = False
```

Если установлен флаг *"use_fully_qualified_names = False"*, то при входе в систему имя доменного пользователя нужно указывать без указания домена!

– во вкладке ***Пользователь*** отображается информация об учетной записи пользователя выбранной рабочей станции и список устройств, назначенных данному пользователю (рисунок 5.31);

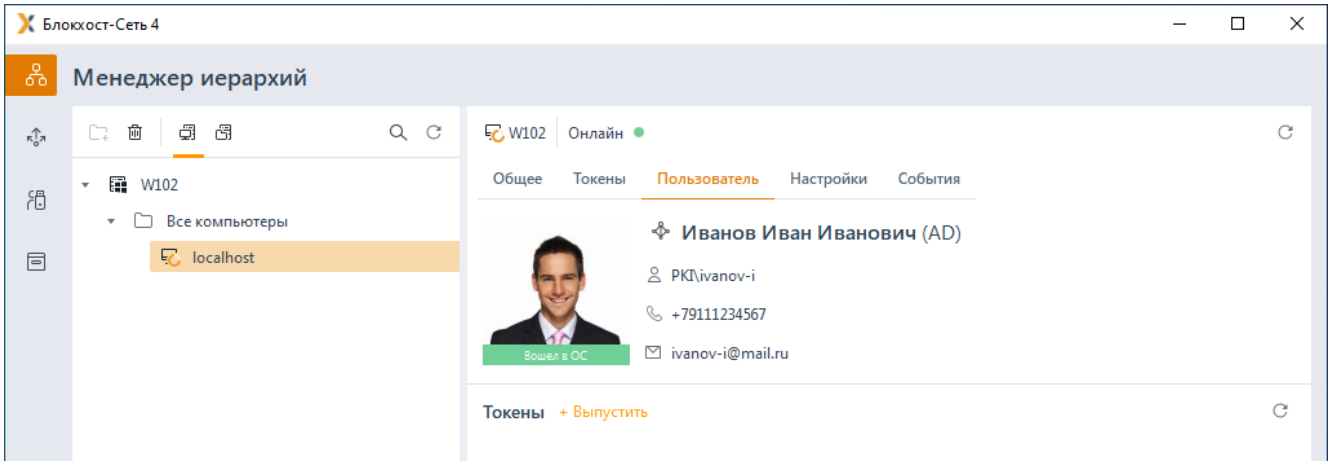


Рисунок 5.31 – Отображение пользователя выбранной рабочей станции

Если на выбранной рабочей станции нет пользователей, осуществивших вход в ОС, во вкладке ***Пользователь*** появится предупреждение об отсутствии активных доменных пользователей на рабочей станции (рисунок 5.32).

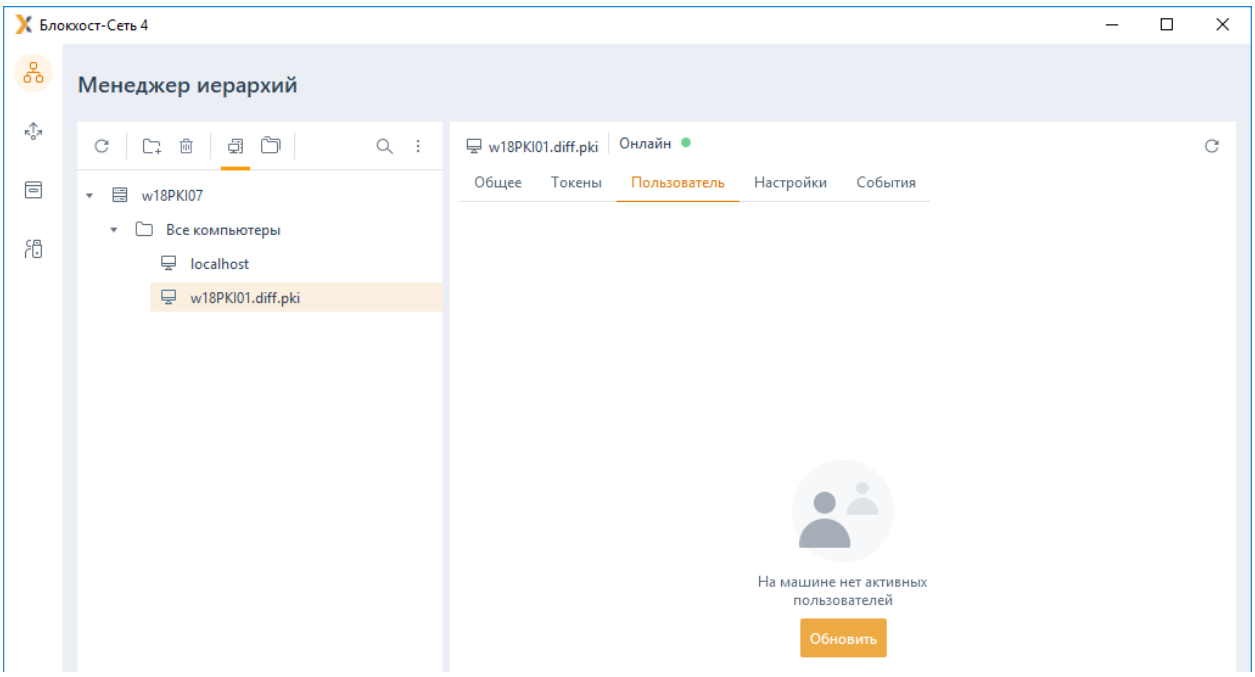


Рисунок 5.32 – Отсутствие доменных пользователей на выбранной рабочей станции

Во вкладках ***Токены/Пользователь*** администратору доступны:

– назначение токена пользователю:

- для входа по управляемому сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный средствами подсистемы управления токенами);
- для входа по стороннему сертификату (на токен записывается цифровой сертификат для аутентификации пользователя при входе, выпущенный

сторонними средствами);

- для безопасного входа по паролю (при использовании токена для аутентификации по паролю, записанному на устройство);
- для учета;

– привязка/отвязка пользователя SafeNode;

– приостановка и возобновление использования токена;

– вывод токена из использования;

– изъятие токена.

При отсутствии активных пользователей на рабочей станции (рисунок 5.32), администратору также доступны все функциональные возможности подсистемы жизненного цикла токенов. Работа по назначению, приостановке и изъятию токенов осуществляется во вкладке ***Токены***.

Выполнение обозначенных действий, описано в соответствующих разделах **Назначение токена пользователю, Приостановка и возобновление использования токена, Вывод токена из использования и Изъятие токена.**

Необходимо учитывать, что удаленное назначение токена для входа по управляемому сертификату на клиентских рабочих станциях под управлением РЕД ОС не работает на экране блокировки и экране входа в систему.

5.5.1 Особенности выпуска токена при удаленном назначении

При удаленном назначении токена для входа по управляемому/стороннему сертификату и для безопасного входа по паролю потребуется ввод PIN-кода пользователя на клиентской рабочей станции (рисунок 5.33).

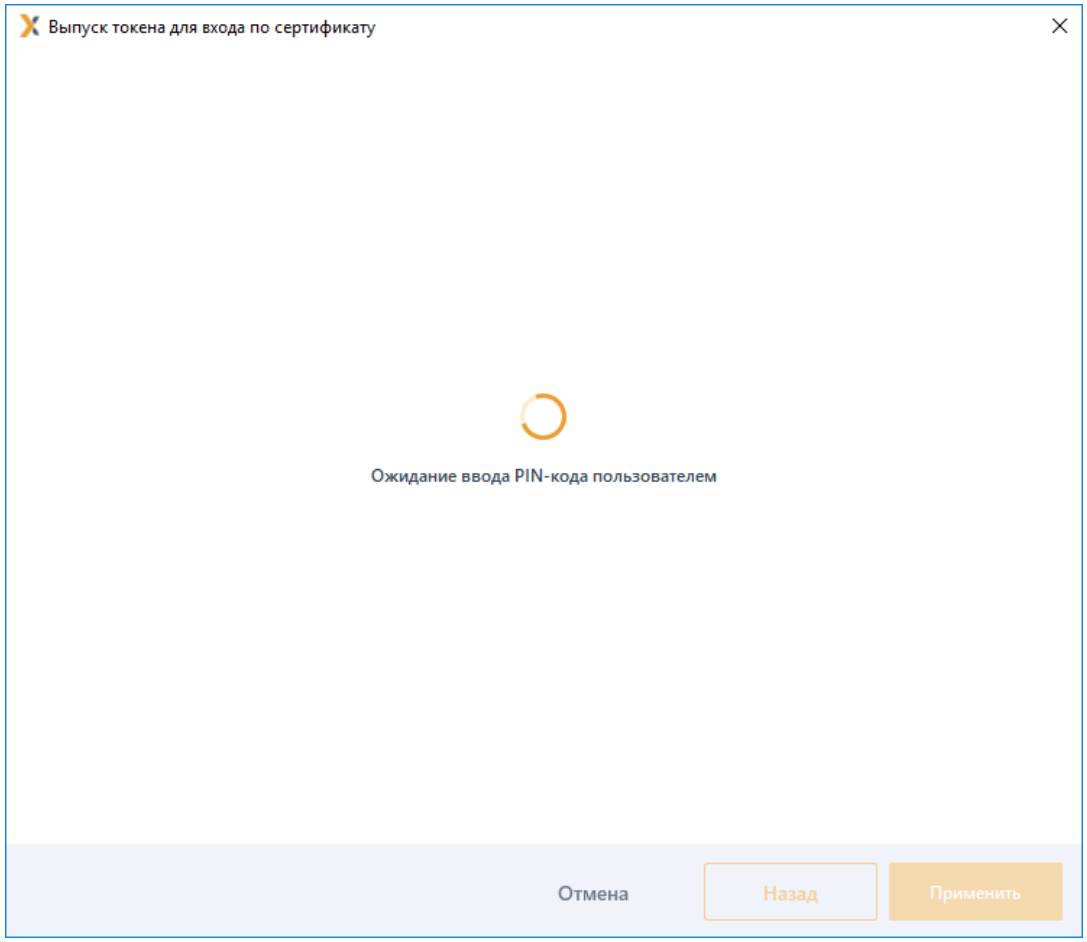


Рисунок 5.33 – Ожидание ввода PIN-кода пользователя

На рабочей станции пользователя появится окно ввода PIN-кода (рисунок 5.34).

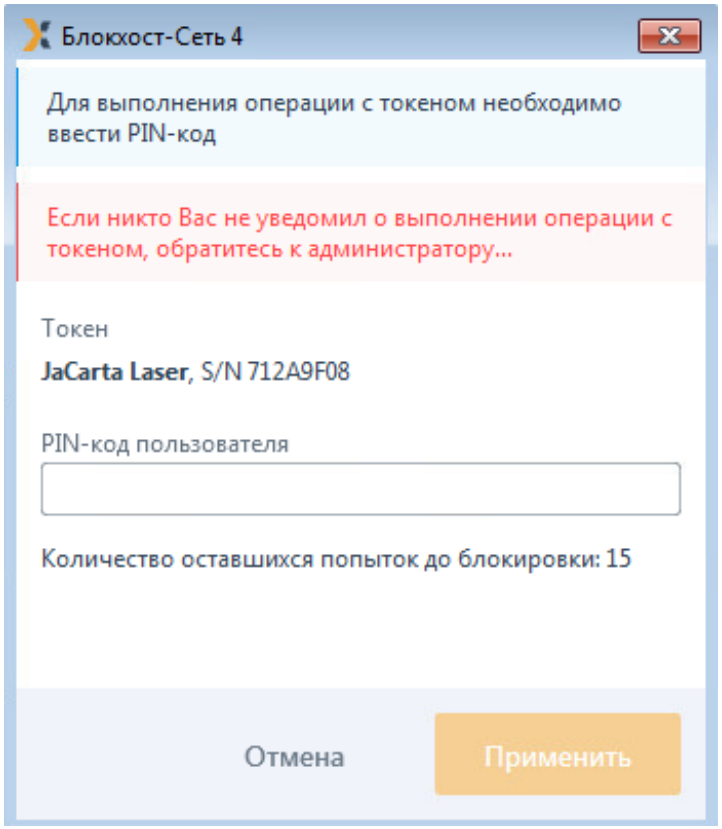


Рисунок 5.34 – Ввод PIN-кода пользователя на клиентской рабочей станции

В ряде ошибочных ситуаций при которых невозможен вход пользователя в ОС, запрос ввода PIN-кода пользователя на клиентской рабочей станции осуществляется до входа в ОС при аутентификации пользователя (рисунок 5.35).

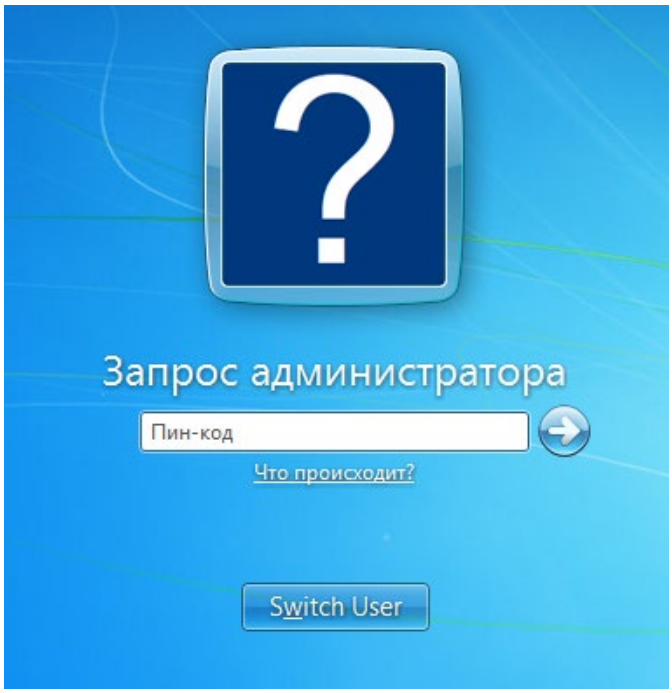


Рисунок 5.35 – Запрос PIN-кода пользователя администратором

В случае успешного ввода PIN-кода появится окно подтверждения корректности введенного PIN-кода (рисунок 5.36) и операция назначения токена пользователю продолжится (рисунок 5.9, 5.21).

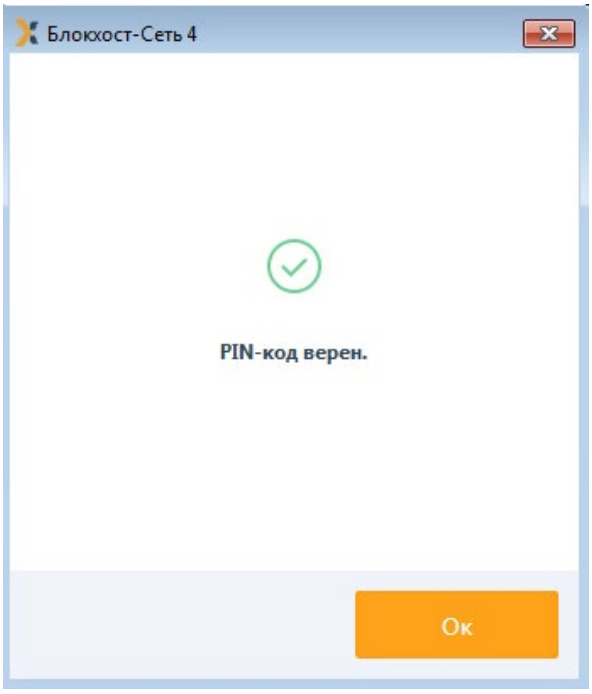


Рисунок 5.36 – Подтверждение корректности PIN-кода пользователя

При возникновении ошибочных ситуации (например, при извлечении токена или отмены выпуска токена администратором) на клиентской рабочей станции появится сообщение об отмене выпуска токена (рисунок 5.37).

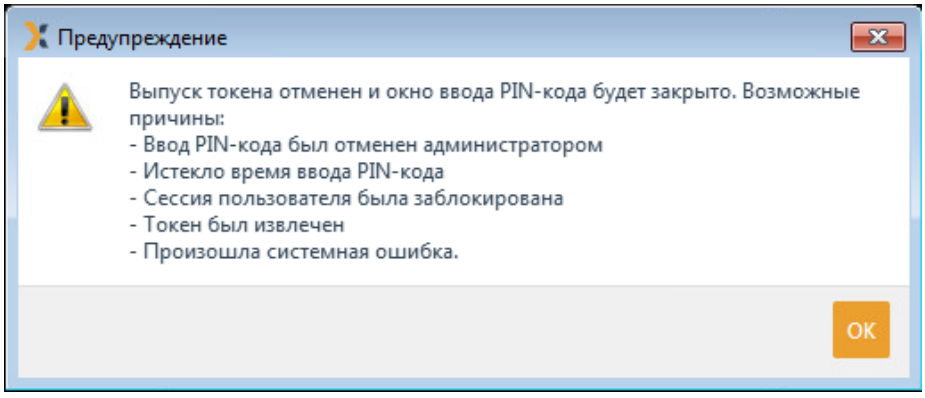


Рисунок 5.37 – Отмена выпуска токена и закрытие окна ввода PIN-кода пользователя

При истечении времени ожидания ответа от клиентской рабочей станции, на АРМ администратора появится сообщение о таймауте ввода PIN-кода пользователя (рисунок 5.38). Администратор может повторить запрос к клиентской рабочей станции в ожидании ответа от пользователя или отменить выпуск токена.

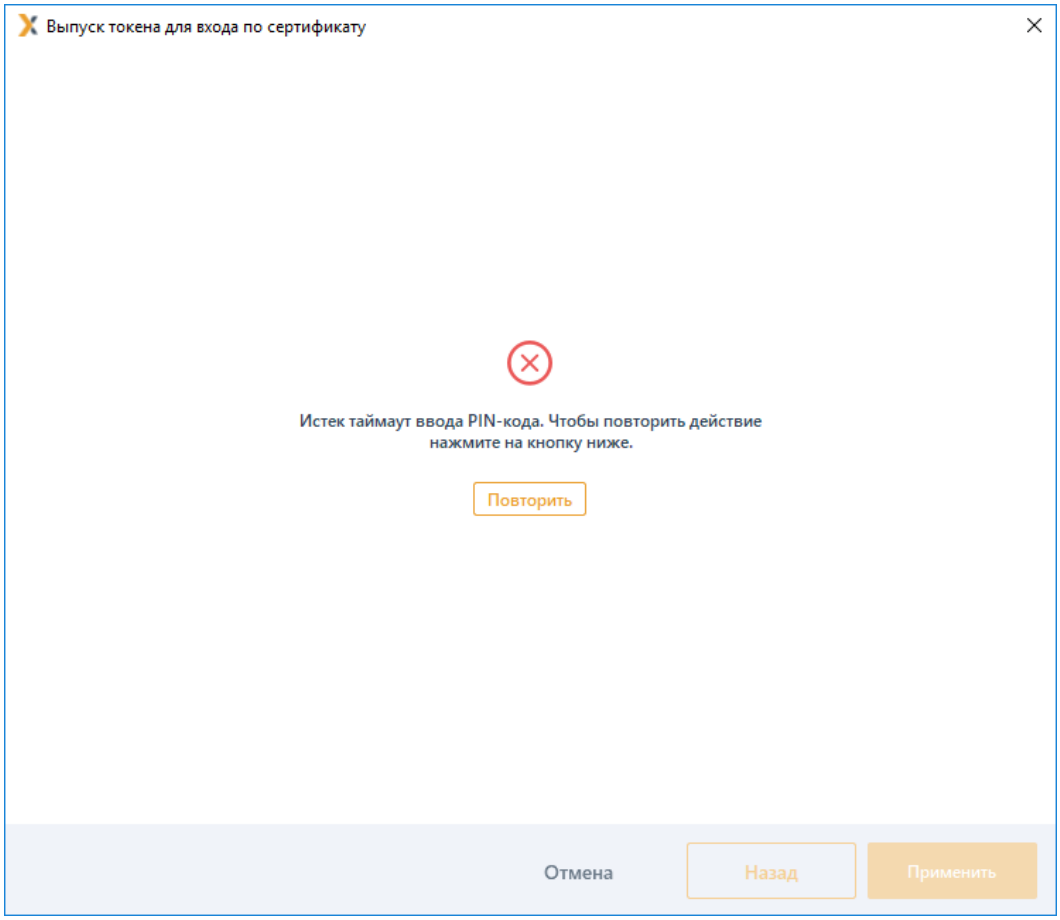


Рисунок 5.38 – Истечение времени ввода PIN-кода пользователя

6 Сертификаты на устройстве

Сертификаты, находящиеся на токене, отображаются:

– в списке токенов во вкладке ***Токены*** после поиска (рисунок 4.17);

– в списке подключенных токенов (рисунок 4.5);

– в профиле пользователя, в области назначенных пользователю токенов, раскрыв токен с сертификатами (рисунок 6.1).

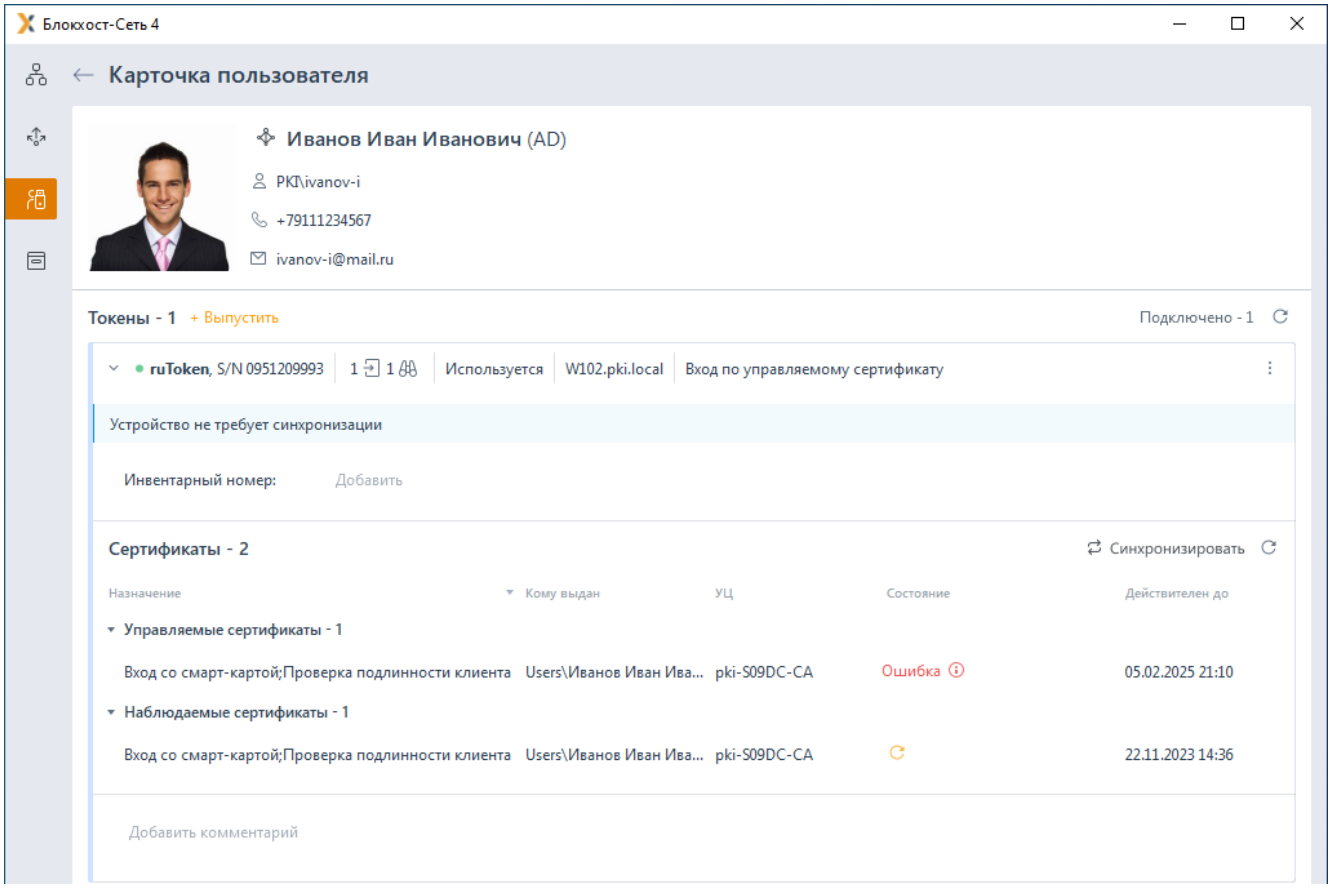


Рисунок 6.1 – Отображение сертификатов на токене

В области ***Токены*** (рисунок 6.1) отображается количество цифровых сертификатов на токене, при этом выделены:

– сертификаты Блокхост-Сети «1» - управляемые сертификаты, выданные средствами подсистемы управления токенами и использующиеся для входа пользователя в систему;

– сторонние сертификаты «1» - наблюдаемые сертификаты, выданные сторонними средствами и использующиеся для электронной подписи в юридически-значимом документообороте или для аутентификации при входе пользователя.

Индикация «» означает появление нового сертификата на выбранном токене, отсутствующего в подсистеме.

Индикация «» означает удаление сертификата уже имеющегося в подсистеме на выбранном токене.

При наведении курсора мыши появляется дополнительная подсказка для администратора (рисунок 6.2).

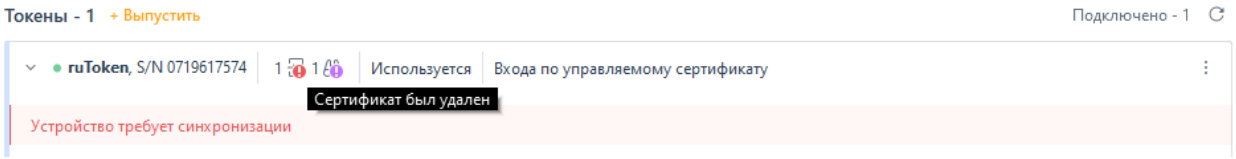


Рисунок 6.2 – Информация о сертификатах на токене

По каждому сертификату отображается информация (рисунок 6.1):

– ***Назначение*** – перечень возможностей, доступных пользователю при использовании данного сертификата;

– ***Кому выдан*** – наименование пользователя, которому был выдан данный сертификат;

– ***УЦ*** – наименование удостоверяющего центра, выдавшего сертификат его владельцу;

– ***Состояние*** – состояние сертификата (перечень возможных состояний приведен в разделе **Состояния сертификата**);

– ***Действителен до*** – срок действия сертификата.

6.1 Состояния сертификата

Состояние сертификата на токене формируется из проверок:

– срока действия сертификата;

– соединения с центром сертификации;

– действий администратора по отношению к данному сертификату.

Состояния, в которых может находится сертификат представлены в таблице 6.1.

Таблица 6.1 – Описание возможных состояний сертификата

Состояние сертификата	Описание
Действительный	Срок действия сертификата не истек. Сертификат пригоден для использования
Отозван	Сертификат отозван окончательно и более не пригоден для

	использования. Окончательный отзыв происходит в результате отзыва устройства или его изъятия.
Временно отозван	Действие сертификата приостанавливается на период выключения устройства. После включения устройства сертификат снова становится действительным.
Истекает	Срок действия сертификата подходит к концу. Необходимо выполнить обновление сертификата, если планируется его дальнейшее использование
Истек	Срок действия сертификата закончился. Сертификат не пригоден для использования.
Ошибка	Состояние сертификата не удалось определить. Центр сертификации недоступен. Сертификат не пригоден для использования

6.2 Жизненный цикл токена с выпуском управляемого сертификата

Жизненный цикл токена с выпуском управляемого сертификата представлен на рисунке 6.3.

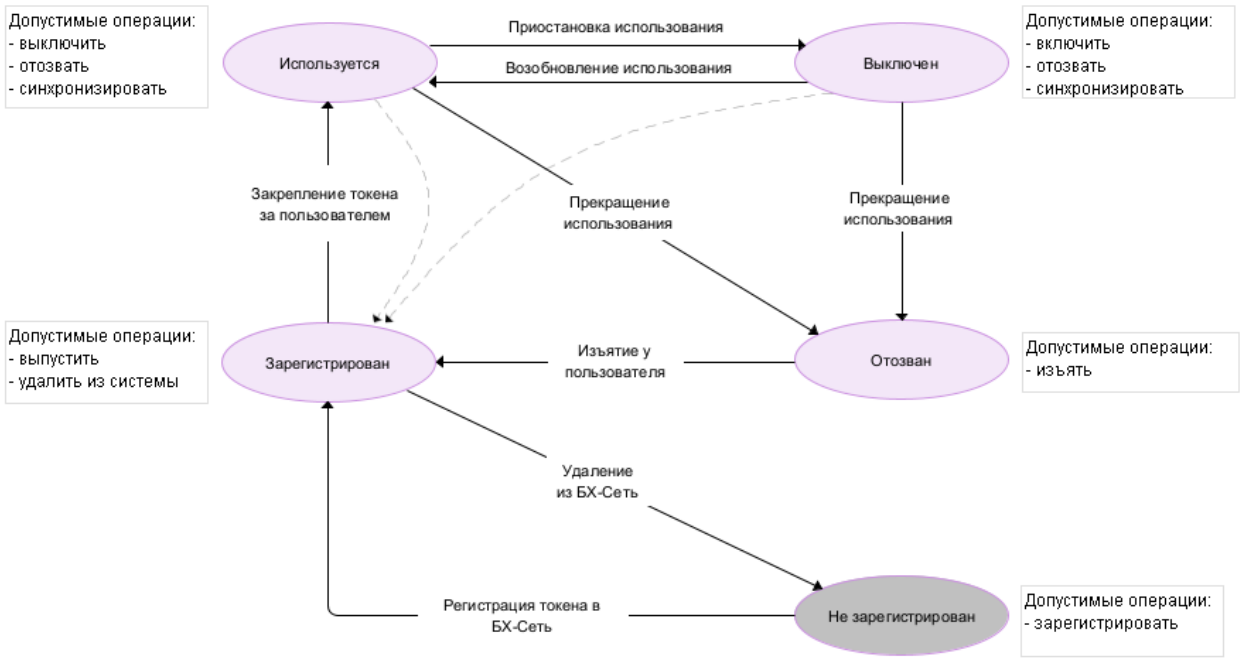


Рисунок 6.3 – Жизненный цикл токена с выпуском управляемого сертификата

Возможные состояния токена, содержащего управляемый сертификат, и доступные действия с ним представлены в таблице 6.2.

Таблица 6.2 – Возможные состояния токена и доступные действия с ним

Состояние	Описание состояния токена	Доступные действия с токеном
Не зарегистрирован	Подключен напрямую к компьютеру, но не зарегистрирован в подсистеме	- Регистрация токена в подсистеме (см. раздел **Добавление токена в подсистему**)
Зарегистрирован	Добавлен в подсистему	- Назначение токена пользователю

		(раздел **Назначение токена пользователю**) - Удаление токена из подсистемы (см. раздел **Удаление токена**)
Используется	Назначен пользователю	- Приостановка использования токена (см. раздел **Приостановка и возобновление использования токена**) - Синхронизация содержимого токена (см. раздел **Синхронизация**) - Вывод токена из использования (см. раздел **Вывод токена из использования**)
Выключен	Использование временно приостановлено	- Возобновление использования токена (см. раздел **Приостановка и возобновление использования токена**) - Синхронизация содержимого токена (см. раздел **Синхронизация**) - Вывод токена из использования (см. раздел **Вывод токена из использования**)
Отозван	Выведен из использования	- Возврат токена в эксплуатацию (см. раздел **Изъятие токена**)

6.2.1 Приостановка и возобновление использования токена

Токен, назначенный пользователю (в состоянии ***Используется***), возможно временно отключить. Приостановка использования токена позволяет отключить токен на определенный промежуток времени, например, на время отпуска пользователя.

Для выключения токена найдите необходимый токен во вкладке ***Токены*** по заданным параметрам поиска или выполните поиск по пользователю во вкладке ***Пользователи***.

Перейдите в строку с токеном, использование которого необходимо приостановить.

Выберите в контекстном меню ***Выключить*** (рисунок 6.4).

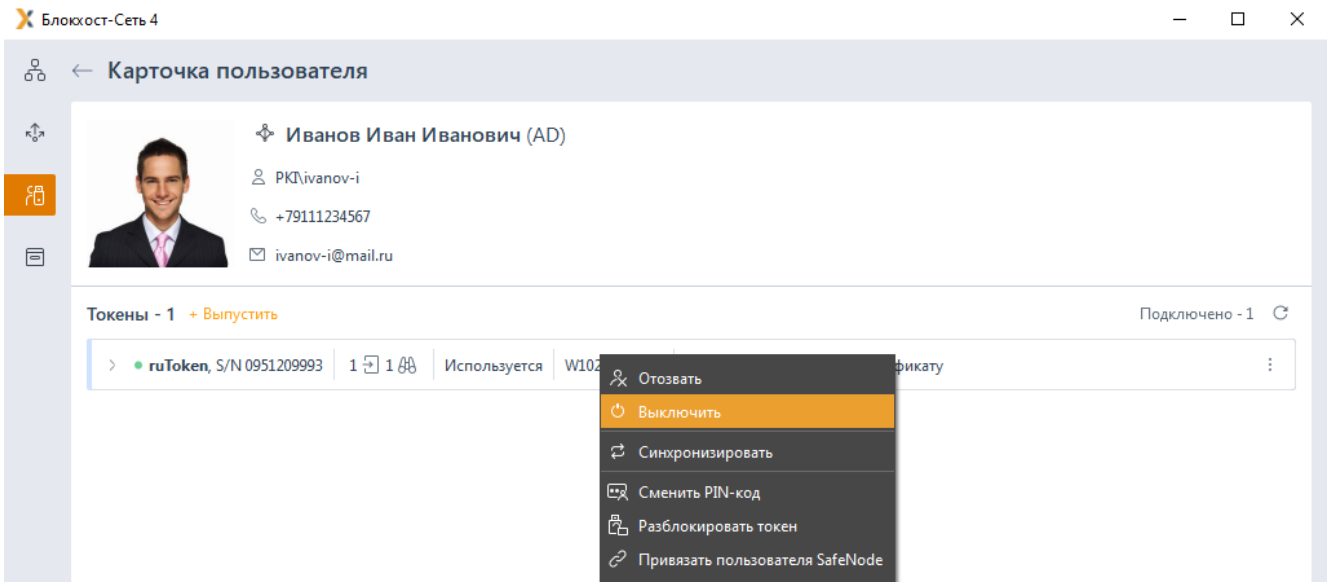


Рисунок 6.4 – Выключение токена

Подтвердите операцию выключения устройства по кнопке ***Да*** в появившемся окне (рисунок 6.55).

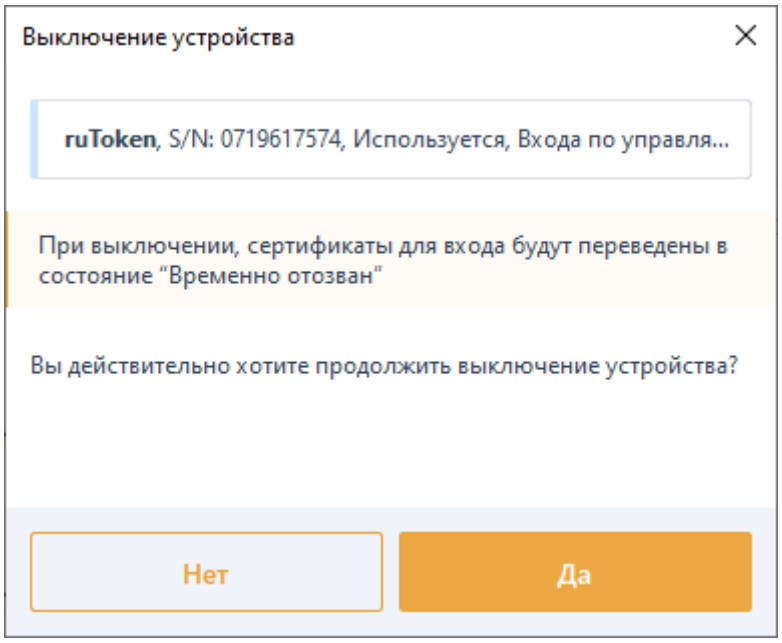


Рисунок 6.5 – Подтверждение выключения токена

Отключенный токен примет состояние ***Выключен*** (рисунок 6.6). Использование токена приостановлено.

Приостановка и возобновление использования токена не требует подключения токена к компьютеру.

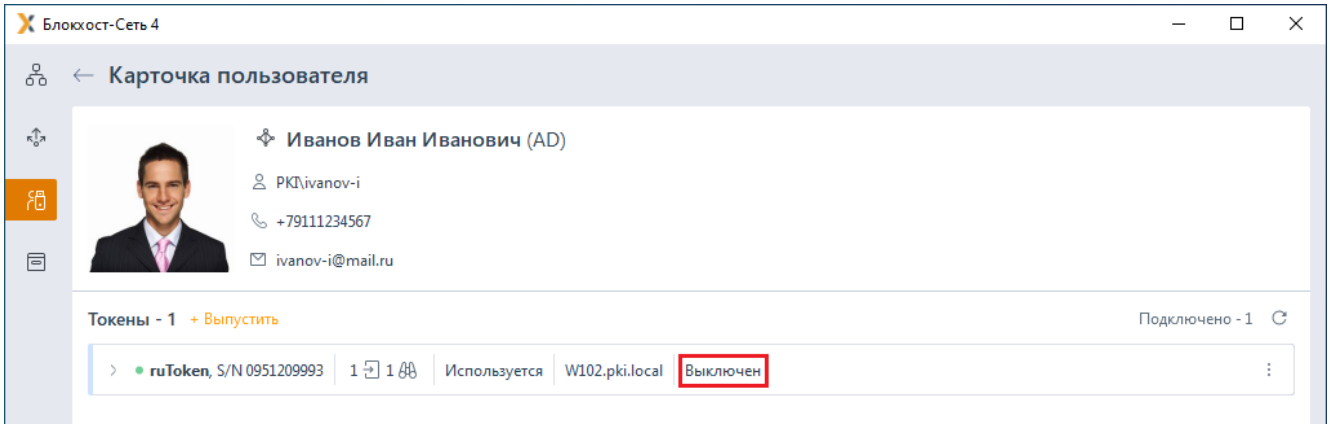


Рисунок 6.6 – Отображение выключенного токена

Для возобновления использования токена произведите аналогичные действия с выбором в контекстном меню кнопки ***Включить*** (рисунок 6.7).

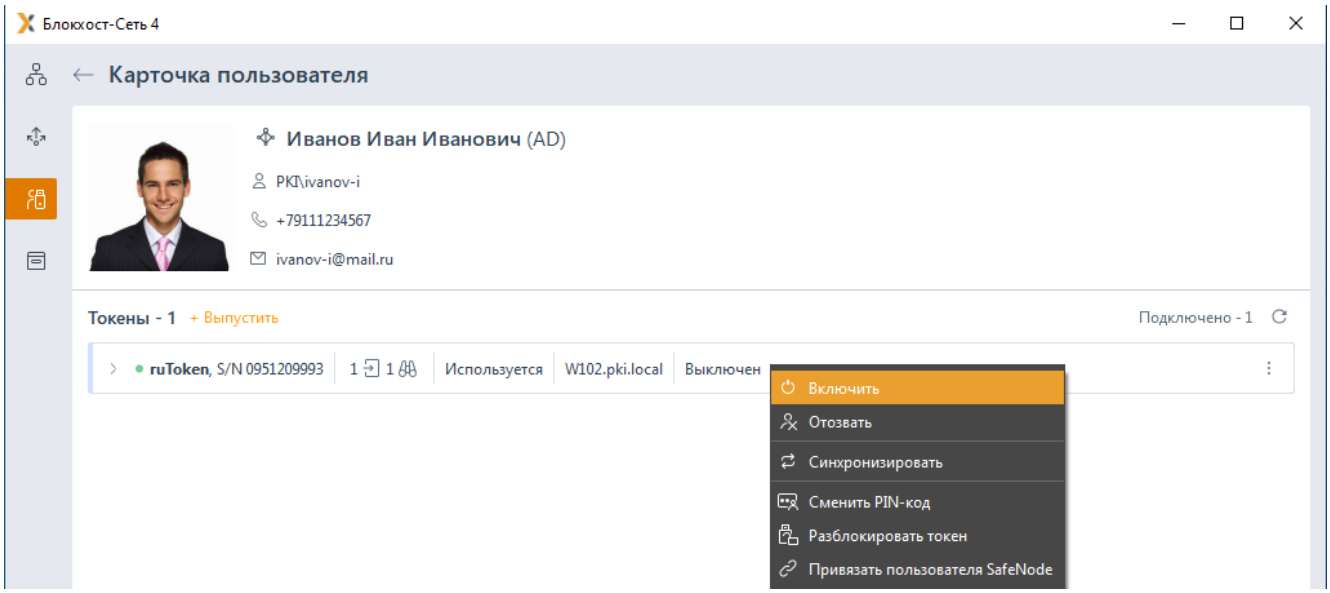


Рисунок 6.7 – Включение токена

6.2.2 Вывод токена из использования

Токен, назначенный пользователю в состояниях ***Используется*** или ***Выключен*** возможно вывести из использования. Токен выводится из использования в случае утери или в случае его неисправности.

При выводе токена из использования, все сертификаты, записанные на него, отзываются без возможности восстановления.

Для отзыва токена найдите необходимый носитель во вкладке ***Токены*** по заданным параметрам поиска или выполните поиск токена по пользователю во вкладке ***Пользователи***.

Перейдите в строку с токеном, который необходимо вывести из использования.

Выберите в контекстном меню ***Отозвать*** (рисунок 6.8).

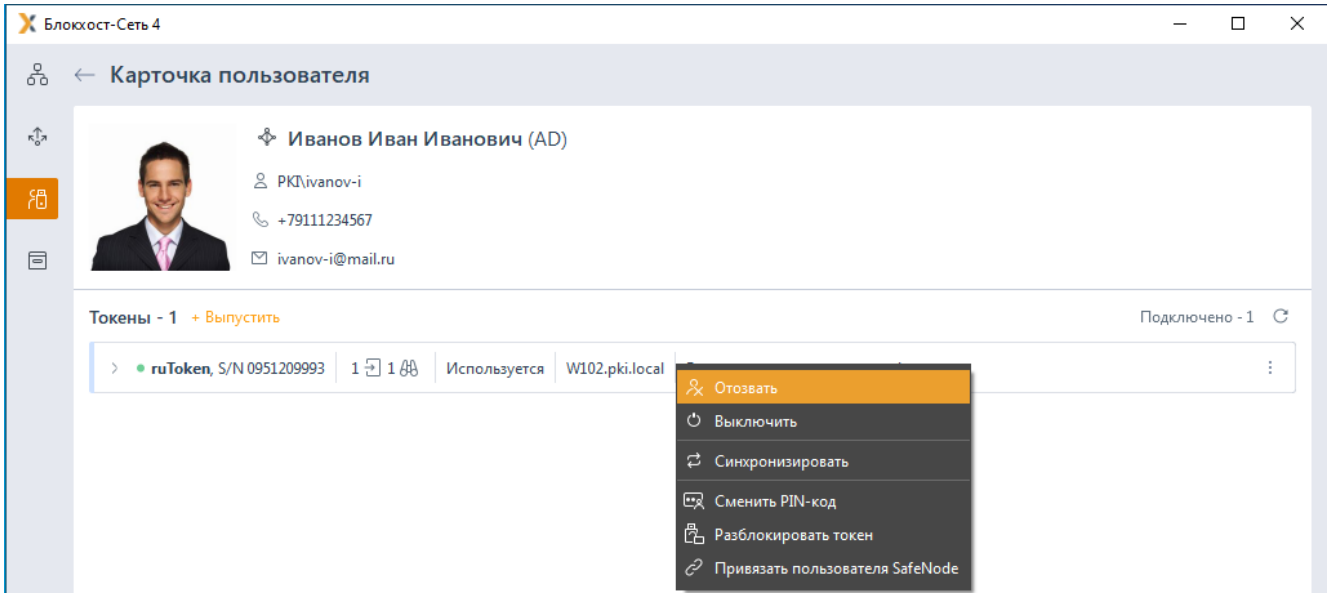


Рисунок 6.8 – Отзыв токена

Подтвердите операцию отзыва устройства по кнопке ***Да*** в появившемся окне (рисунок 6.9).

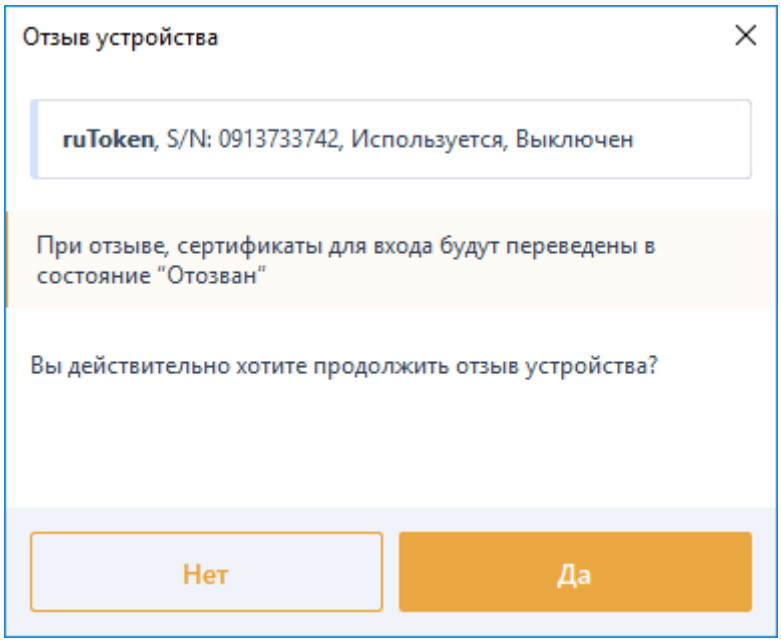


Рисунок 6.9 – Подтверждение отзыва токена

Отозванный токен примет состояние ***Отозван*** (рисунок 6.10). Использование токена невозможно.

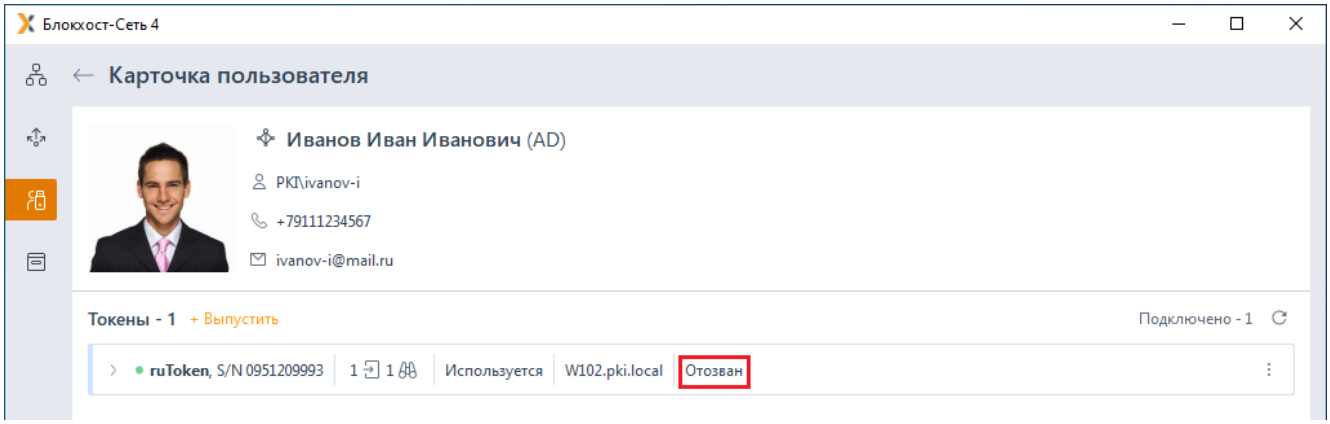


Рисунок 6.10 – Отображение отозванного токена

6.2.3 Изъятие токена

Выведенный из использования токен (в состоянии ***Отозван***), возможно вернуть в эксплуатацию для последующего назначения пользователю с записью новых сертификатов.

Отозванный токен остается закреплен за пользователем, которому назначен. При изъятии токена, привязка токена к пользователю удаляется и токен становится доступен для назначения.

Для изъятия отозванного токена найдите необходимый токен во вкладке ***Токены*** по заданным параметрам поиска или выполните поиск токена по пользователю во вкладке ***Пользователи***.

Перейдите в строку с токеном, который необходимо изъять и вернуть в эксплуатацию.

Выберите в контекстном меню ***Изъять*** (рисунок 6.11).

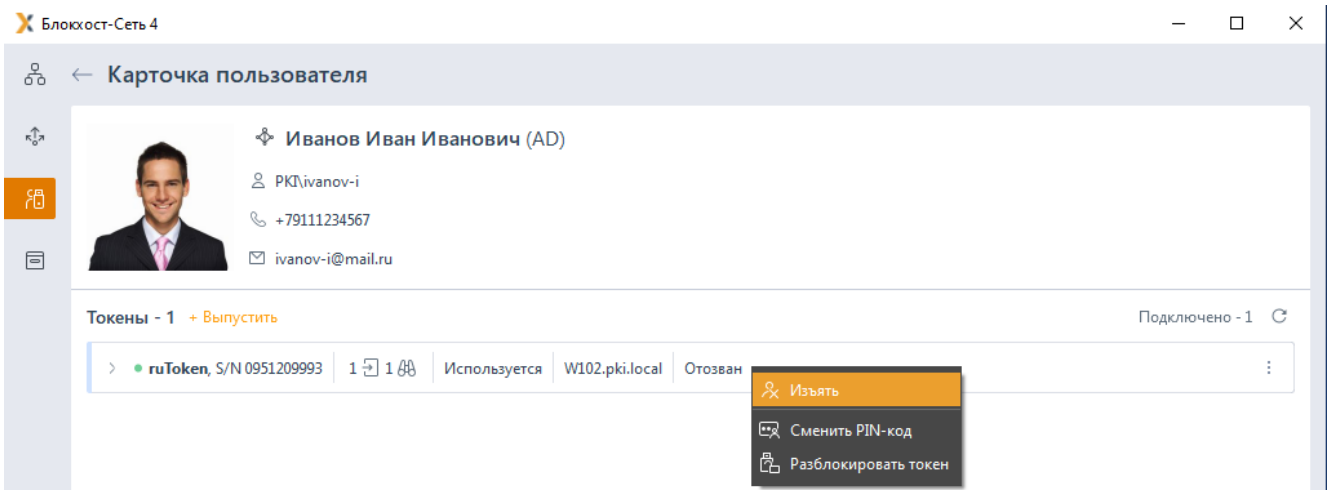


Рисунок 6.11 – Изъятие токена

Подтвердите операцию изъятия устройства по кнопке ***Да*** в появившемся окне (рисунок 6.12).

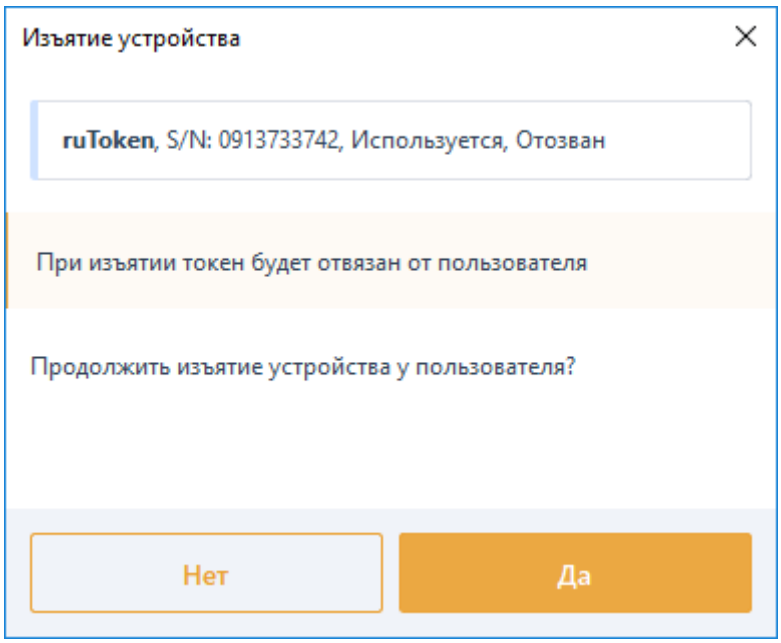


Рисунок 6.12 – Подтверждение изъятия токена

Изъятый токен примет состояние ***Зарегистрирован*** (рисунок 6.13). Токен доступен для дальнейшей эксплуатации и назначения пользователю.

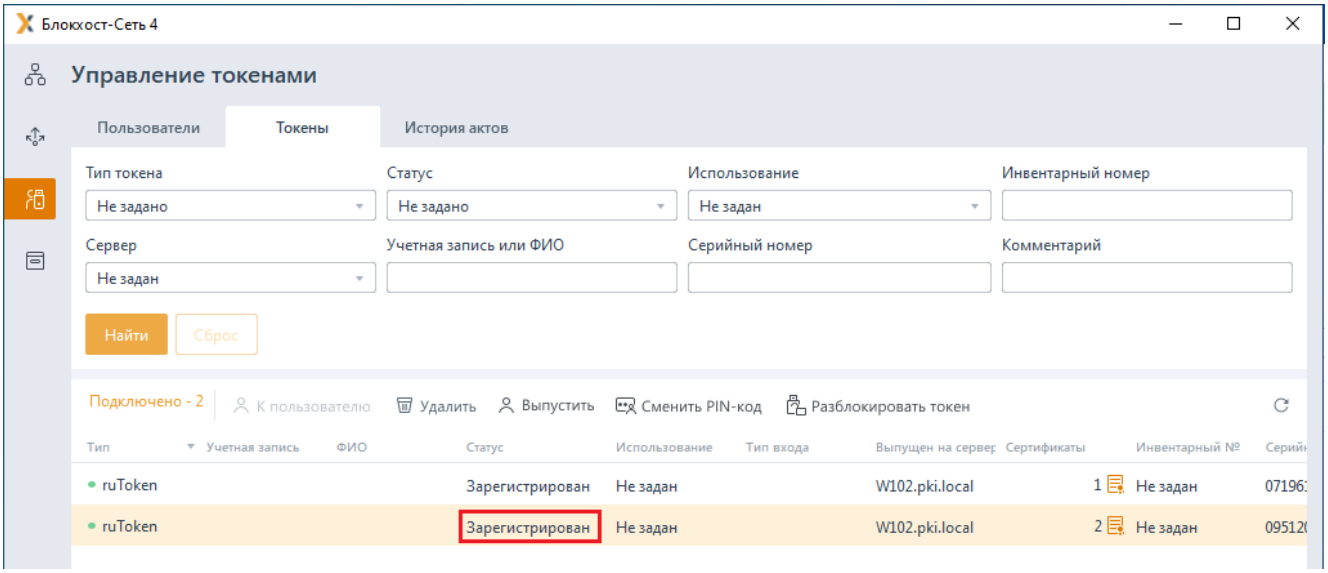


Рисунок 6.13 – Возврат токена в эксплуатацию

6.2.4 Аварийное изъятие токена

Аварийное изъятие токена позволяет изъять токен, назначенный пользователю, если по какой-либо причине установка соединения с центром сертификации невозможна. При этом токен изымается без выполнения операции отзыва/временного отзыва сертификата для входа.

Для аварийного изъятия токена при выполнении операций выключения или отзыва токена стандартным способом в появившемся окне с сообщением об ошибке (рисунок 6.14) нажмите ***Изъять аварийно***.

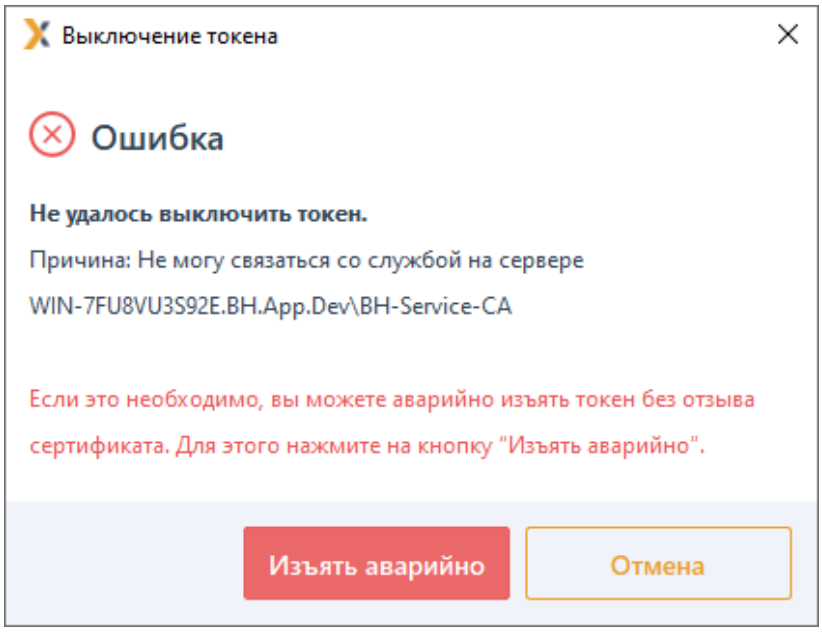


Рисунок 6.14 – Аварийное изъятие токена

Изъятый токен примет состояние ***Зарегистрирован*** (рисунок 6.13). Токен доступен для дальнейшей эксплуатации и назначения пользователю.

6.3 Жизненный цикл токена без выпуска управляемого сертификата

Жизненный цикл токена без выпуска управляемого сертификата, представлен на рисунке 6.15.

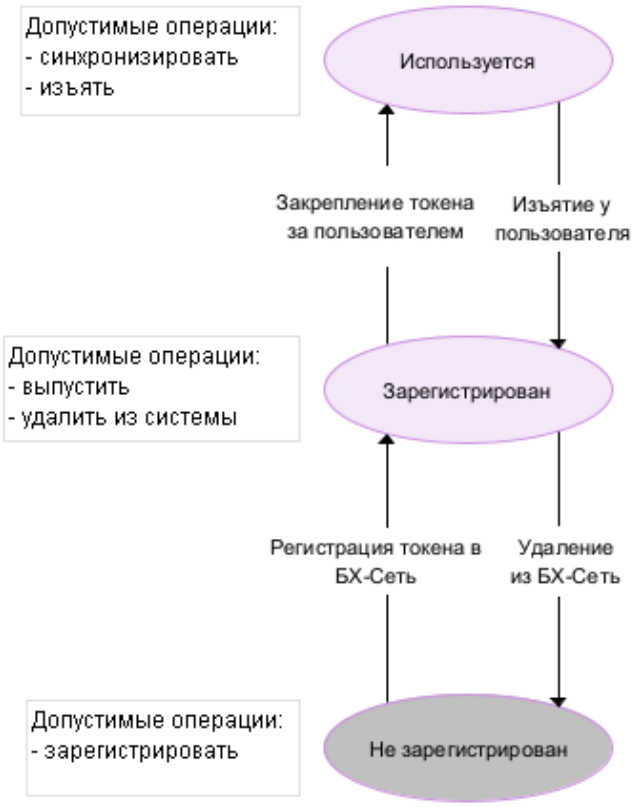


Рисунок 6.15 – Жизненный цикл токена без выпуска сертификата

В отличие от токена с выпуском сертификата, токен без управляемого сертификата может быть только зарегистрирован в подсистеме и назначен пользователю. Приостановка и отзыв токена в данном случае невозможны.

Возможные состояния токена без управляемого сертификата и доступные действия с ним представлены в таблице 6.3.

Таблица 6.3 – Возможные состояния токена без управляемого сертификата и доступные действия с ним

Состояние	**Описание**	**Возможные действия**
Не зарегистрирован	Подключен напрямую к компьютеру, но не зарегистрирован в подсистеме	- Регистрация токена в подсистеме (см. раздел **Добавление токена в подсистему**)
Зарегистрирован	Добавлен в подсистему	- Назначение токена пользователю (раздел **Назначение токена пользователю**) - Удаление токена из подсистемы (см. раздел **Удаление токена**)
Используется	Назначен пользователю	- Синхронизация токена (см. раздел **Синхронизация токена**) - Вывод токена из использования (см. раздел **Вывод токена из использования**)

7 Синхронизация

Синхронизация позволяет сопоставить фактическое содержимое токена с базой данных подсистемы управления жизненным циклом токенов.

Для проведения синхронизации токен должен быть назначен пользователю (в состоянии ***Используется***) или приостановлен (в состоянии ***Выключен***).

При возникновении расхождений содержимого токена с базой данных подсистемы, появится сообщение о необходимости проведения синхронизации (рисунок 7.1).

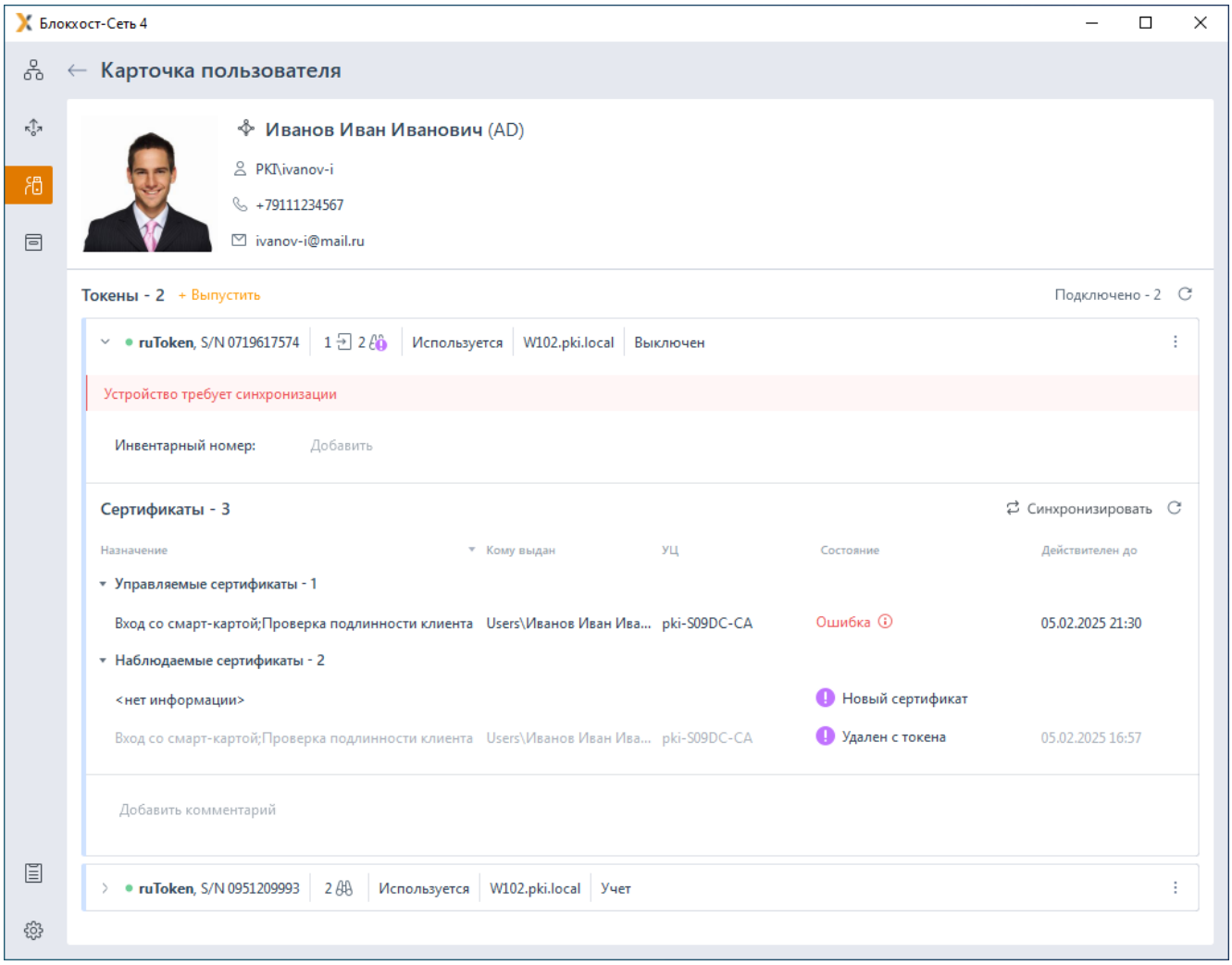


Рисунок 7.1 – Устройство требует синхронизации

Синхронизация запускается:

– выбором пункта ***Синхронизировать*** в контекстном меню (рисунок 7.2);

– по кнопке Синхронизировать в области назначенных пользователю токенов, раскрыв необходимый токен.

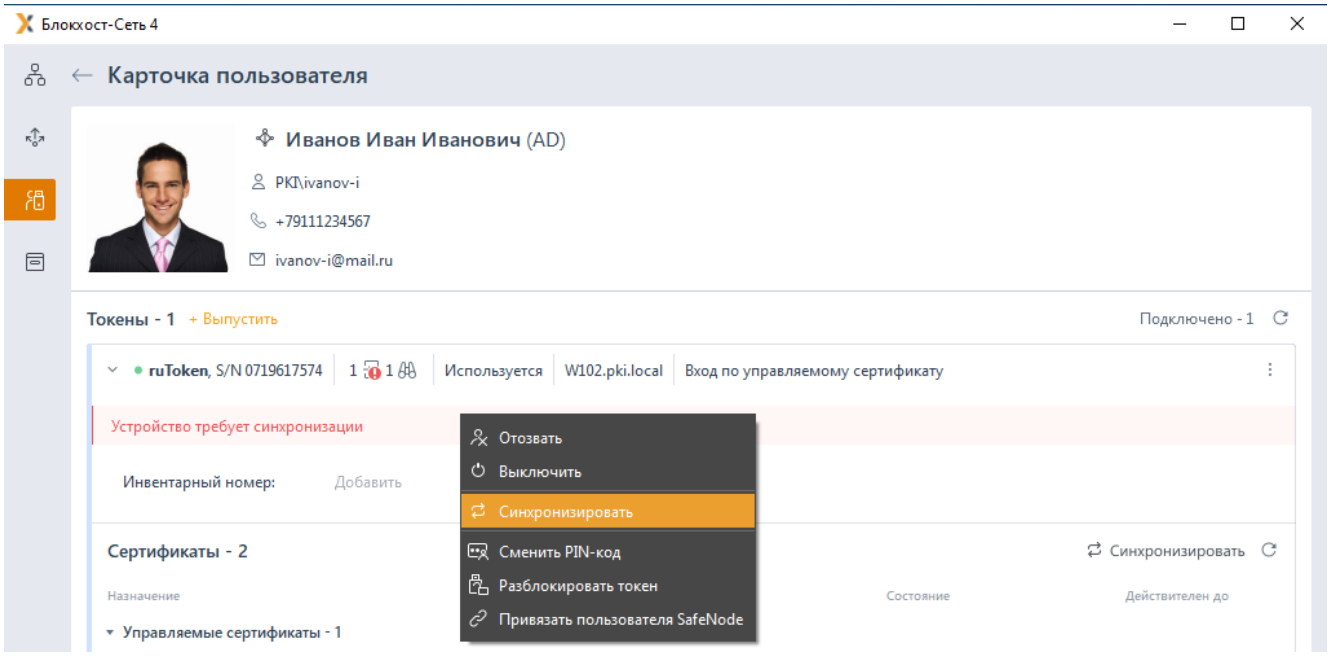


Рисунок 7.2 – Выбор операции синхронизации

В окне синхронизации перечислены действия с сертификатами на токене, которые будут выполнены при синхронизации (рисунок 7.3).

Действия при выполнении синхронизации различаются в зависимости от назначения токена и от средств, с помощью которых выпущены сертификаты на токене (собственных или сторонних организаций).

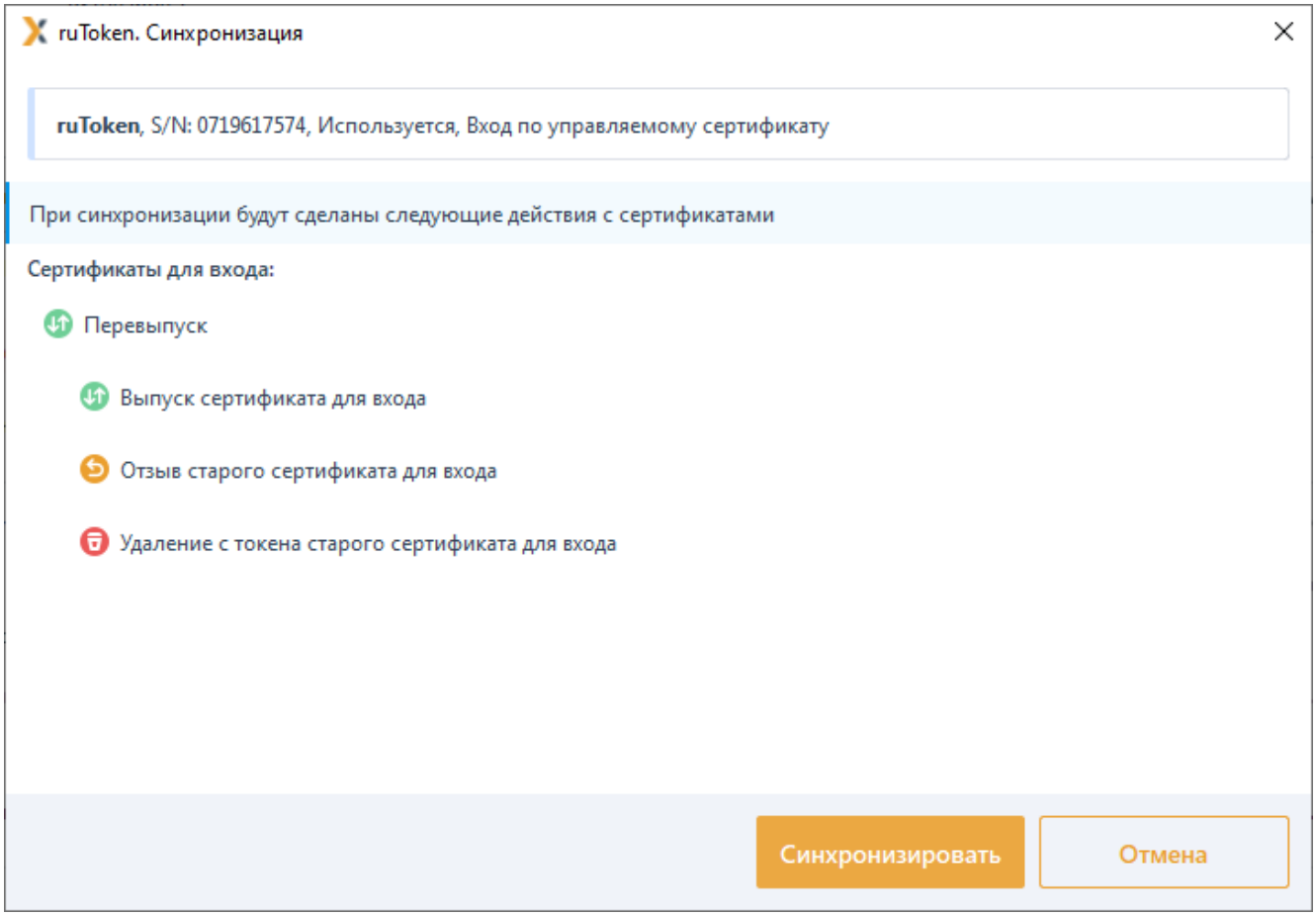


Рисунок 7.3 – Процесс синхронизации

При нажатии кнопки ***Синхронизировать*** потребуется ввод PIN-кода токена (рисунок 7.4).

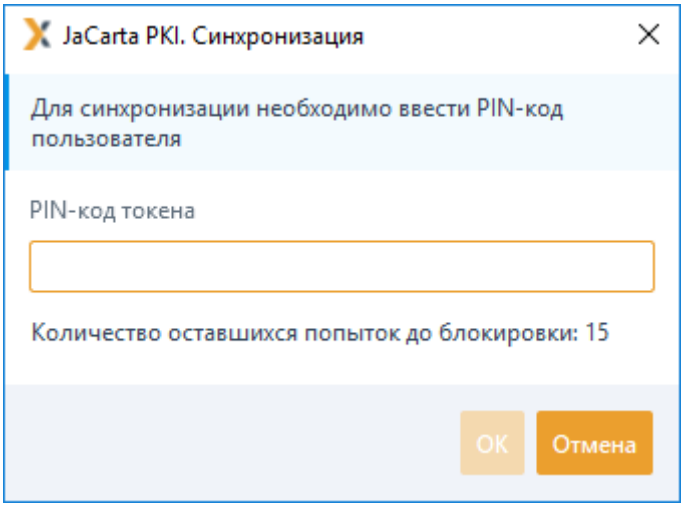


Рисунок 7.4 – Ввод PIN-кода при синхронизации

Если операция синхронизации выполняется удаленно с АРМ администратора при этом токен, который необходимо синхронизировать, подключен к клиентской

рабочей станции, потребуется ввод PIN-кода пользователя на клиентской рабочей станции (рисунок 5.31). На АРМ администратора появится сообщение об ожидании ввода PIN-кода пользователя (рисунок 5.32).

По завершению процесса синхронизации, появится окно с сообщением об успешном завершении операции (рисунок 7.5).

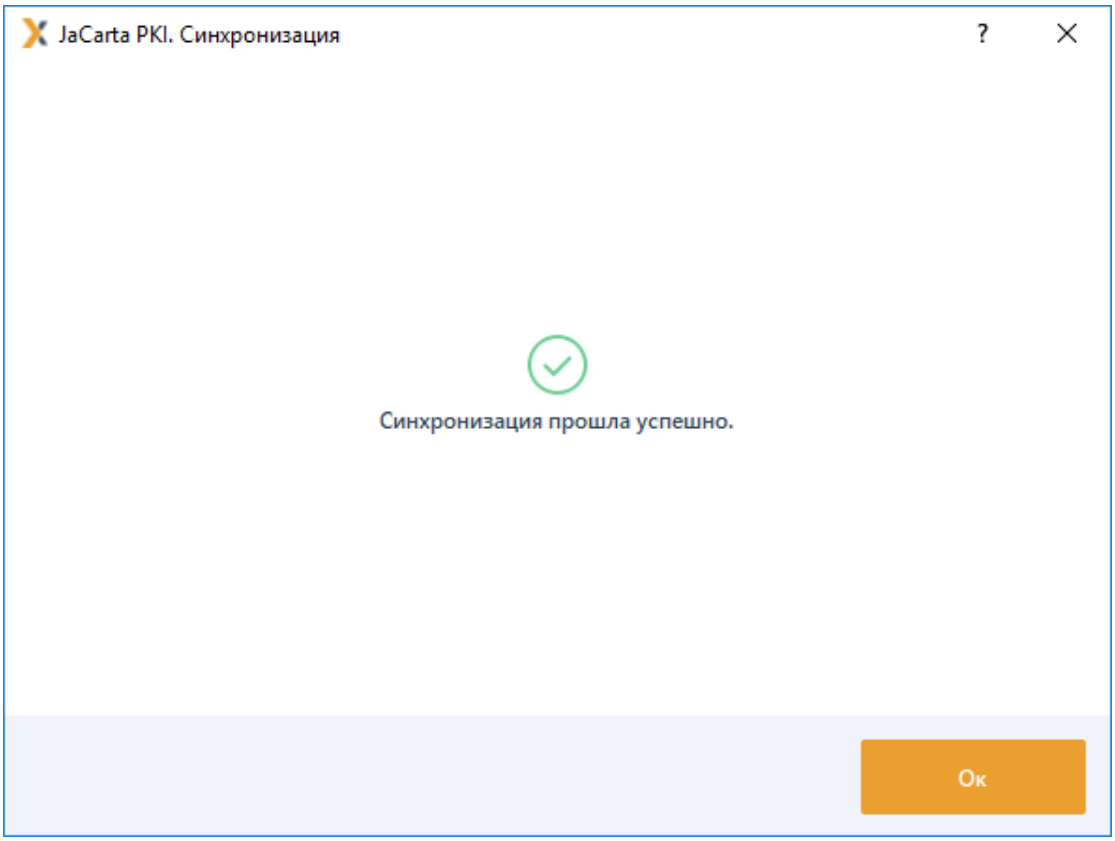


Рисунок 7.5 – Успешное завершение процесса синхронизации

В области назначенных пользователю токенов, появится сообщение, что синхронизация устройства больше не требуется (рисунок 7.6).

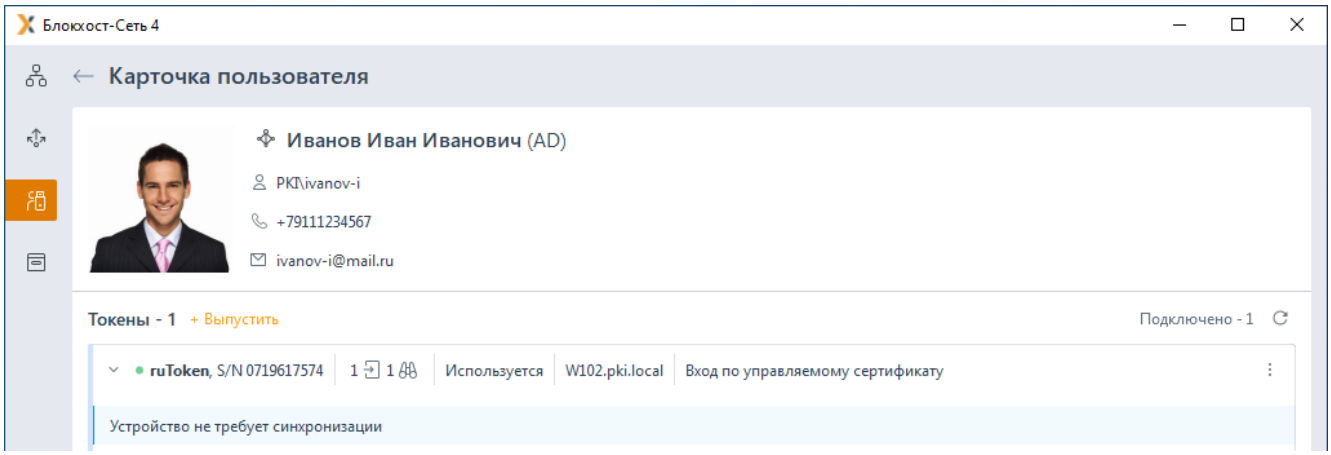


Рисунок 7.6 – Устройство не требует синхронизации

7.1 Синхронизация сертификатов для входа, выпущенных подсистемой

Действия в процессе синхронизации токенов, содержащих сертификаты для входа, выпущенные средствами подсистемы жизненного цикла представлены в таблице 7.1.

Таблица 7.1 – Действия в процессе синхронизации токенов

Состояние токена	**Состояние сертификата на токене**	**Действия в процессе синхронизации**
Используется	Действительный	Синхронизация не требуется
	Истекает	- Выпускается новый сертификат на замену истекающему. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Заменяемый сертификат отзывается, удаляется с токена и из подсистемы.
	Истек	- Выпускается новый сертификат на замену истекшему. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Истекший сертификат отзывается, удаляется с токена и из подсистемы.
	Временно отозван	*Сертификат для входа был отозван внешними средствами.* - Выполняется изменение статуса сертификата и сертификат возвращается из отзыва.
	Отозван	*Сертификат для входа был отозван внешними средствами.* - Выпускается новый сертификат на замену отозванному. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Отозванный сертификат удаляется с токена и из подсистемы.
	Нет сертификата	*На токене отсутствует сертификат для входа (удален внешними средствами).* - Выпускается новый сертификат. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Если на момент синхронизации в подсистеме зарегистрирован удаленный с токена сертификат, он удаляется.
Выключен	Действительный	*Сертификат на токене в состоянии **Выключен** должен*

		*находиться в состоянии **Временно отозван** (состояние изменено внешними средствами).* - Выполняется временный отзыв сертификата.
	Истекает	*Сертификат на токене в состоянии **Выключен** должен находиться в состоянии **Временно отозван** (состояние изменено внешними средствами).* - Выпускается новый сертификат на замену истекающему сертификату. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Новый сертификат временно отзывается. - Заменяемый сертификат отзывается, удаляется с токена и из подсистемы.
	Истек	*Сертификат на токене в состоянии **Выключен** должен находиться в состоянии **Временно отозван** (состояние изменено внешними средствами).* - Выпускается новый сертификат на замену истекшему. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Новый сертификат временно отзывается. - Истекший сертификат удаляется с токена и из подсистемы.
	Временно отозван	Синхронизация не требуется
	Отозван	*Сертификат на токене в состоянии **Выключен** должен находиться в состоянии **Временно отозван** (состояние изменено внешними средствами).* - Выпускается новый сертификат на замену отозванному. - Новый сертификат записывается на токен и регистрируется в подсистеме. - Новый сертификат временно отзывается. - Отозванный сертификат удаляется с токена и из подсистемы.
	Нет сертификата	*На токене отсутствует сертификат для входа (удален внешними средствами).* - Выпускается новый сертификат. - Новый сертификат записывается на токен и регистрируется в подсистеме.

		- Новый сертификат временно отзывается. - Если на момент синхронизации в подсистеме зарегистрирован удаленный с токена сертификат, он удаляется из подсистемы.

7.2 Синхронизация наблюдаемых сертификатов, используемых для входа, выпущенных сторонними средствами

Действия в процессе синхронизации токенов, содержащих сертификаты для входа, выпущенных сторонними средствами представлены в таблице 7.2.

Таблица 7.2 – Действия в процессе синхронизации токенов

Состояние токена	**Состояние сертификата на токене**	**Действия в процессе синхронизации**
Используется	Действительный	На токене содержится сертификат для входа, выпущенный УЦ сторонних организаций (не зарегистрированный в подсистеме). При синхронизации возможны следующие действия: - удалить сертификат с токена; - оставить сертификат на токене (в разделе **Синхронизация наблюдаемых сертификатов, не используемых для входа, выпущенных УЦ сторонних организаций**).
Выключен		

7.3 Синхронизация наблюдаемых сертификатов, не используемых для входа

Подсистема жизненного цикла токенов не производит никаких действий с наблюдаемыми сертификатами, выпущенными сторонних средствами и используемыми в юридическо-значимом документообороте.

Подсистема осуществляет контроль в соответствии с таблицей ниже:

– наличия сертификатов на токене (удален/добавлен);

– состояний сертификатов;

– уведомление пользователей об окончании срока действия сертификатов (истекает/истек).

Таблица 7.3 – Действия в процессе синхронизации токенов

Состояние сертификата на токене в настоящий момент	**Состояние сертификата на токене при предыдущей синхронизации**	**Действия в процессе синхронизации**
Действующий	Действующий	Сертификат контролируется подсистемой.

		Никаких изменений не производится. Состояние сертификата после синхронизации – ***Действующий***
	Сертификат на токене отсутствует	Сертификат ставится на контроль подсистемы. Состояние сертификата после синхронизации – ***Действующий***
Истекает	Действующий	Сертификат контролируется подсистемой. Состояние сертификата после синхронизации – ***Истекает***
Истек	Действующий	Сертификат контролируется подсистемой. Состояние сертификата после синхронизации – ***Истек***
Отозван	Действующий	Сертификат контролируется подсистемой. Состояние сертификата после синхронизации – ***Отозван***
Сертификат на токене отсутствует	Действующий	Сертификат снимается с контроля подсистемы. После синхронизации сертификат удаляется.

7.4 Синхронизация токенов, не содержащих сертификаты

Действия в процессе синхронизации токенов, не содержащих сертификаты, аналогичны действиям при синхронизации наблюдаемых сертификатов, используемых для электронной подписи и описаны в разделе **Синхронизация наблюдаемых сертификатов, не используемых для входа**.

8 Общие настройки

Во вкладке ***Настройки*** в разделе ***«Выпуск сертификатов»*** задаются профили для выпуска сертификатов в том числе параметры сервисной учетной записи для корректной работы подсистемы управления жизненным циклом токенов по выпуску сертификатов (рисунок 8.1).

Подробная установка параметров сервисной учетной записи описана в документах «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA», «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag».

При эксплуатации подсистемы управления жизненным циклом токенов во вкладке ***Выпуск сертификатов*** можно добавлять профили для выпуска сертификатов разных удостоверяющих центров и изменять сервисную учетную запись, сертификат агента регистрации, шаблон сертификата пользователя для входа, при необходимости.

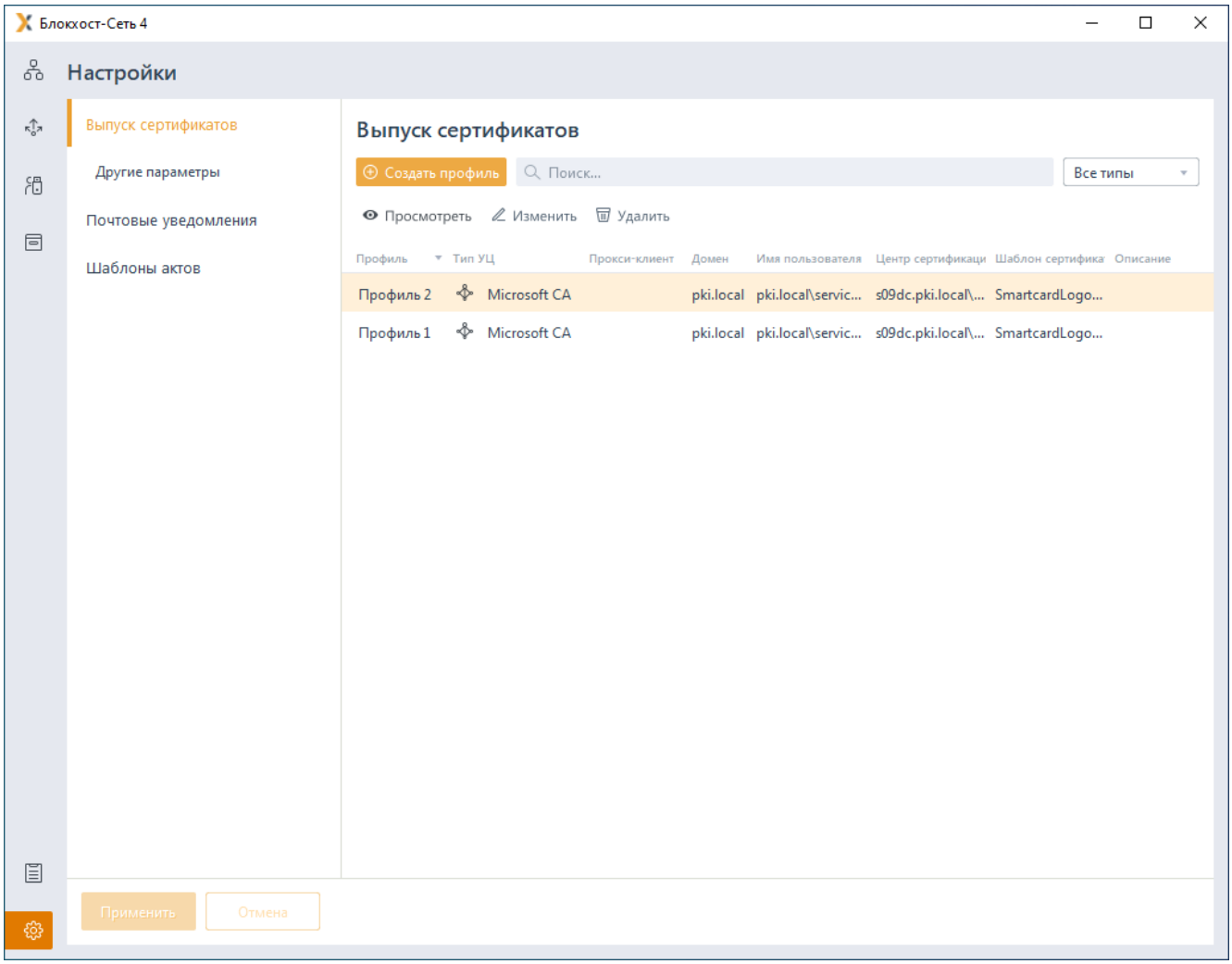


Рисунок 8.1 – Общие настройки

8.1 Настройка дополнительных параметров

Во вкладке ***Настройки*** в разделе ***«Другие параметры»*** задаются параметры вычисления статуса наблюдаемых сертификатов, параметры наименования устройств и настройка срока изменения статуса сертификатов при их истечении (рисунок 8.2).

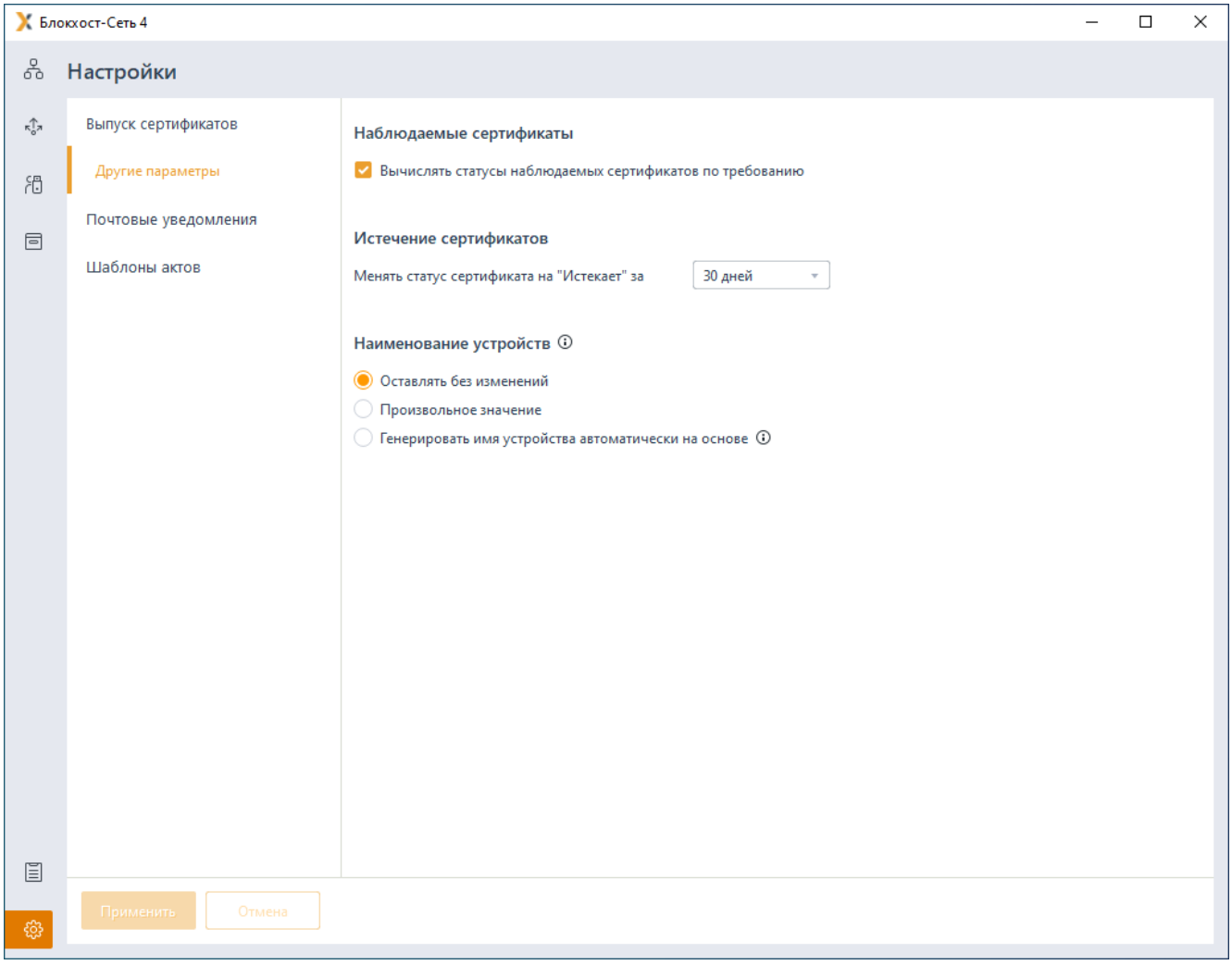


Рисунок 8.2 – Дополнительные настройки

Установленный параметр ***Вычислять статусы наблюдаемых сертификатов по требованию*** позволяет при выполнении операции синхронизации устройства запрашивать актуальный статус сертификатов, выпущенных УЦ сторонних организаций.

В параметре ***Истечение сертификатов*** устанавливается количество дней до окончания срока действия сертификата, за которые у истекающего сертификата необходимо поменять статус на «Истекает».

Параметр ***Наименование устройств*** позволяет задавать значение наименования при регистрации, назначении или инициализации устройства:

– ***Оставлять без изменений*** – наименование, уже присвоенное устройству, остается без изменений.

– ***Произвольное значение*** – наименование устройства задается произвольно, вручную в строке ввода (рисунок 8.3).

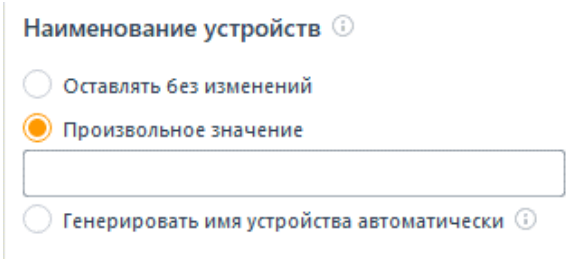


Рисунок 8.3 – Установка произвольного наименования устройства

– ***Генерировать имя устройства автоматически на основе*** – наименование устройства генерируется при выдаче токена пользователю из параметра ***Общее имя (Common Name)*** (рисунок 8.4).

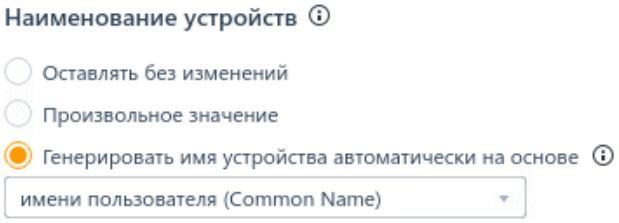


Рисунок 8.4 – Установка автоматической генерации наименования устройства

8.2 Настройка почтовых уведомлений

Подсистема жизненного цикла токенов позволяет настроить рассылку почтовых уведомлений администраторам и пользователям об истекающих/истекших сертификатах на токенах.

8.2.1 Настройка почтового сервера

Для настройки почтового сервера перейдите в консоли по кнопке во вкладку ***Почтовые уведомления*** в раздел ***«Настройки»*** (рисунок 8.5).

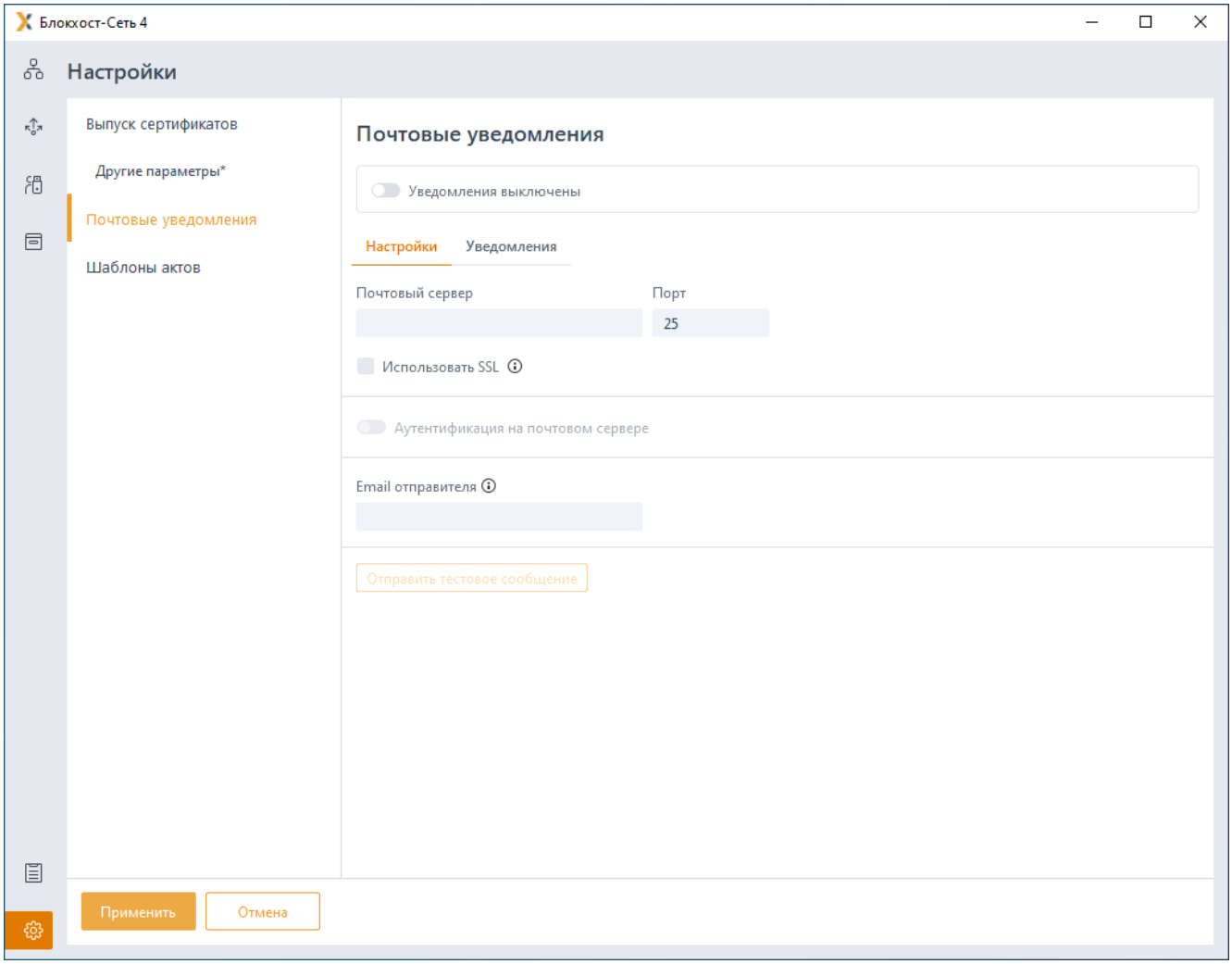


Рисунок 8.5 – Настройка почтового сервера

Включите почтовые уведомления по кнопке 

и задайте настройки почтового сервера в соответствующих полях (рисунок 8.6).

Рисунок 8.6 – Ввод адреса и порта почтового сервера

При необходимости отправки почтовых уведомлений по защищенному каналу SSL установите флаг в параметре ***Использовать SSL***.

При отправке почтовых уведомлений по защищенному каналу SSL, чаще всего используются порты 587 или 465.

При необходимости аутентификации на почтовом сервере, установите переключатель

Аутентификация на почтовом сервере и введите аутентификационные данные в поля ***Имя пользователя*** и ***Пароль*** (рисунок 8.7).

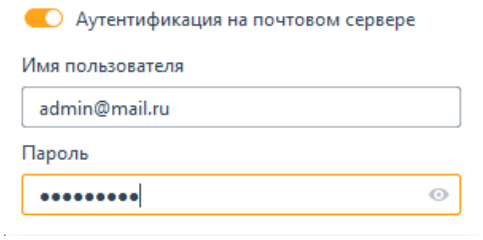


Рисунок 8.7 – Аутентификация на почтовом сервере

При вводе e-mail адреса отправителя в соответствующее поле, получатели будут видеть указанный адрес при получении уведомления в поле ***От кого*** (рисунок 8.8).

Рисунок 8.8 – Ввод e-mail адреса отправителя

Для проверки заданных настроек почтового сервера нажмите ***Отправить тестовое сообщение***, введите адрес получателя и нажмите ***Отправить*** (рисунок 8.9).

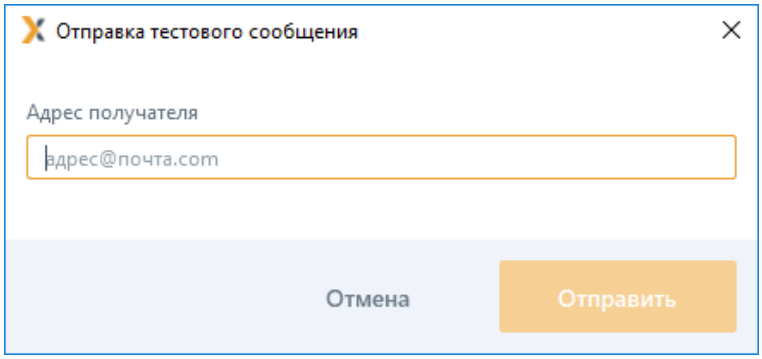


Рисунок 8.9 – Отправка тестового сообщения

При возникновении ошибки отправки тестового уведомления, проверьте корректность введенных настроек почтового сервера и повторите отправку.

8.2.2 Настройка оповещений пользователей

Для настройки оповещений пользователей перейдите по кнопке во вкладку ***Почтовые уведомления*** в раздел ***«Уведомления»*** (рисунок 8.10).

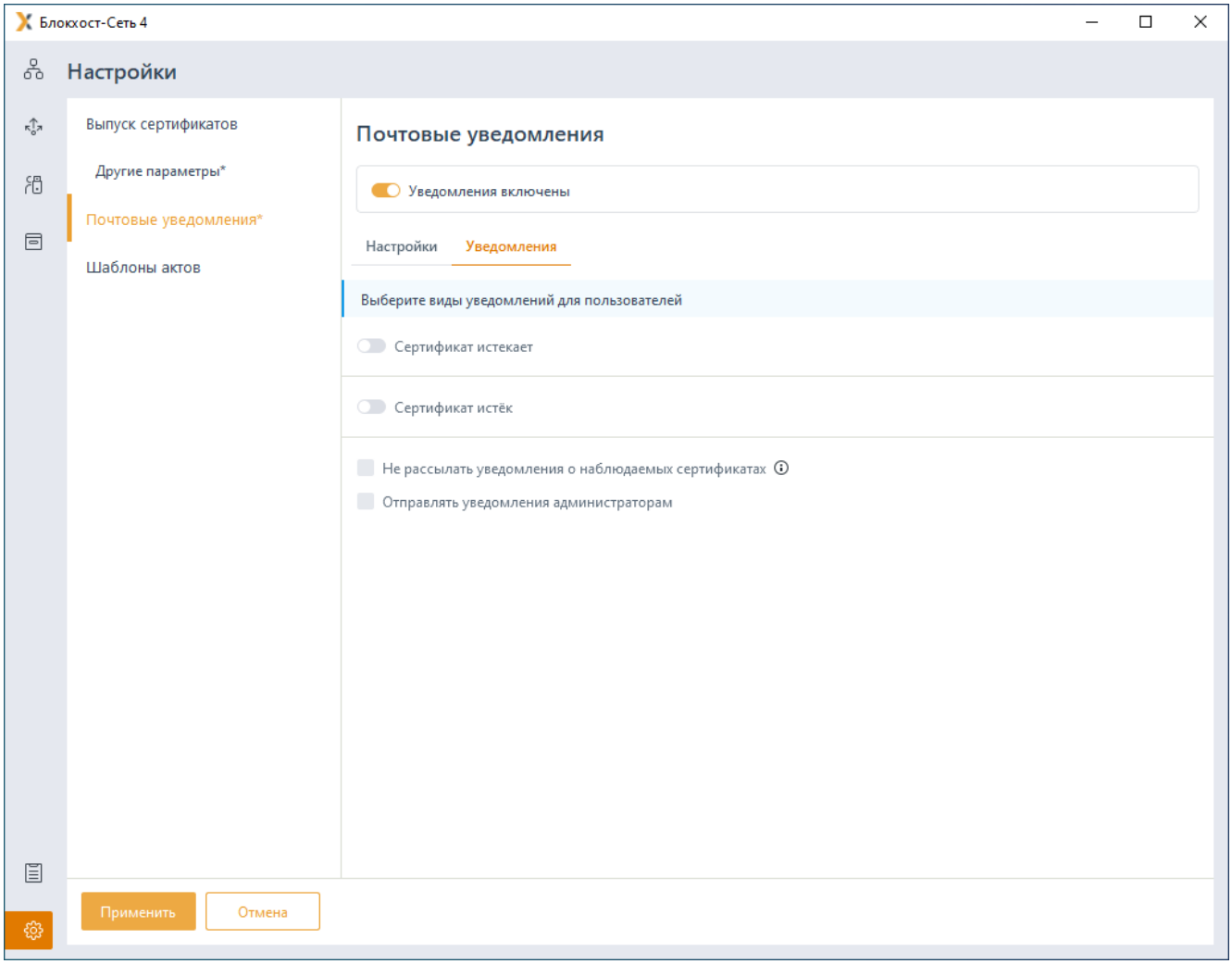


Рисунок 8.10 – Настройка оповещений пользователей

Включите почтовые уведомления по кнопке 

и выберите типы событий, о которых уведомляется пользователь.

Возможно задать оповещения об истекающих и/или истекших сертификатах на токене (рисунок 8.11).

Для отправки пользователю уведомления о выбранном событии необходимо, чтобы в свойствах его учетной записи Active Directory был указан адрес электронной почты.

При выборе уведомлений об истекающих сертификатах установите за какое количество дней требуется уведомить получателя о приближении срока окончания сертификата, и частоту повторения уведомления (рисунок 8.11).

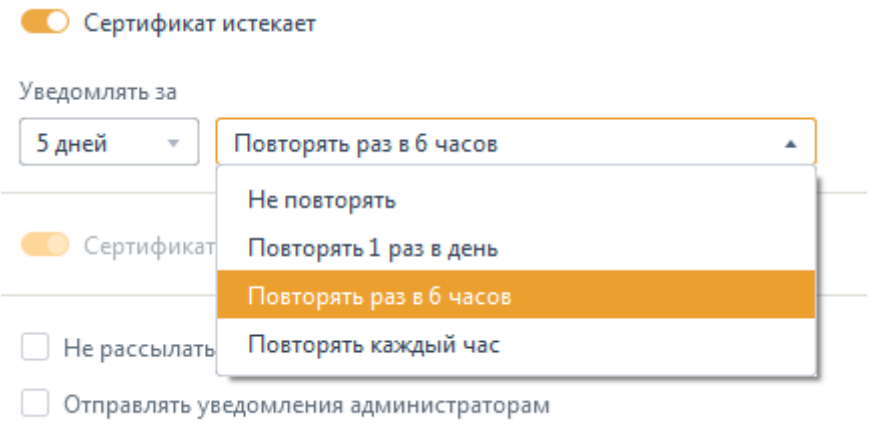


Рисунок 8.11 – Выбор частоты повторения уведомления об истекающем сертификате

Если рассылка уведомлений об истечении сертификатов, выпущенных УЦ сторонних организаций, не требуется, установите параметр ***Не рассылать уведомления о наблюдаемых сертификатах*** (рисунок 8.12).

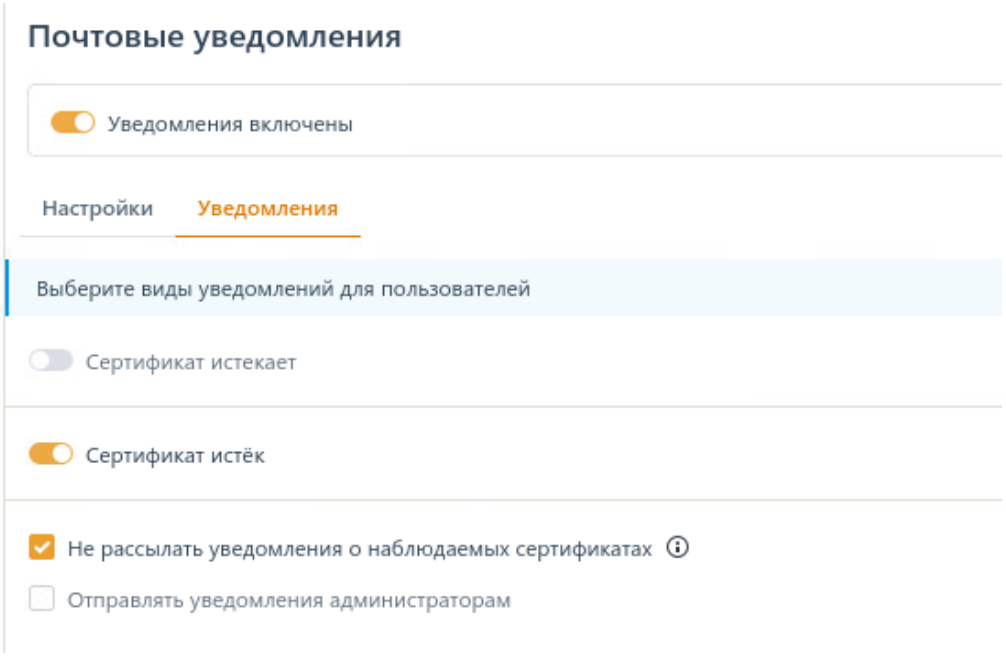


Рисунок 8.12 – Не рассылать уведомления о наблюдаемых сертификатах

При необходимости сообщать о выбранных событиях администраторам, установите параметр ***Отправлять уведомления администраторам*** и введите e-mail адреса всех получателей, разделяя их точкой с запятой (рисунок 8.13).

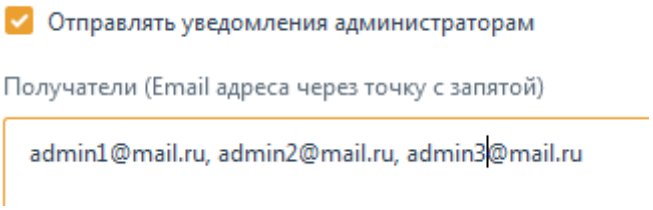


Рисунок 8.13 – Отправление уведомлений перечисленным администраторам

Для сохранения настроек почтовых уведомлений нажмите ***Применить***.

8.3 Шаблоны актов

Во вкладке ***Настройки*** в разделе ***«Шаблоны актов»*** возможно задать или отменить формирование актов при выполнении операций выдачи токена пользователю, синхронизации токена, изъятии токена и удалении токена из системы (все операции, при которых возможно формирование акта, перечислены в таблице 3.1).

Настройка формирования акта при выполнении операции выпуска токена осуществляется путем установки или снятия флага напротив акта (рисунок 8.14).

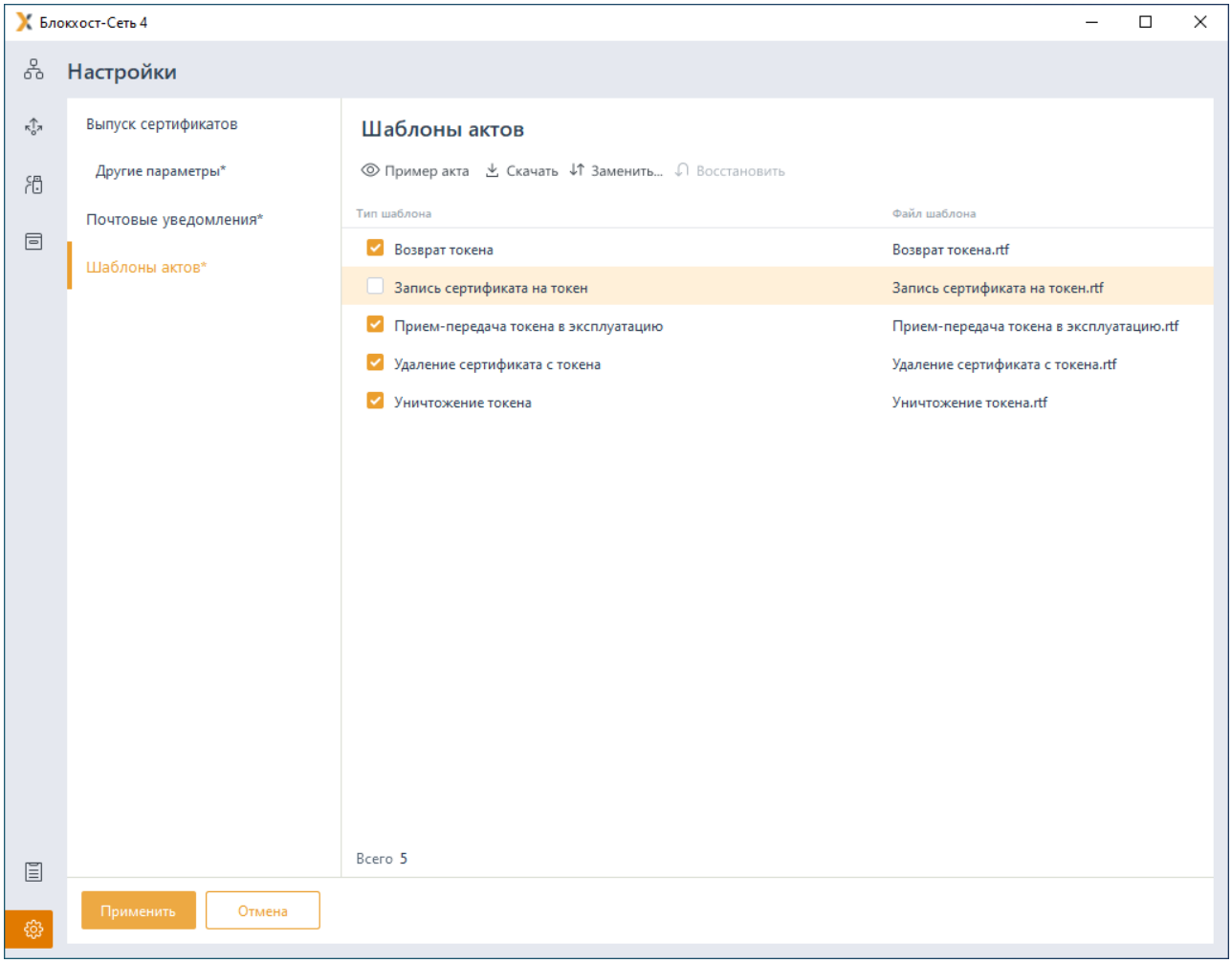


Рисунок 8.14 – Настройка шаблонов печати

8.3.1 Изменение предустановленных шаблонов

Шаблоны, по которым формируются акты, заданы в системе по умолчанию. В таблице 8.1 перечислены все типы шаблонов, по которым возможно формирование актов.

Таблица 8.1 – Типы шаблонов актов

Тип шаблона	Описание шаблона
Возврат токена	Формируется при изъятии токена у пользователя. Содержит номер и дату формирования акта, данные по возвращаемому токену и персональные данные пользователя, у которого произведено изъятие.
Запись сертификата на токен	Формируется при выпуске пользователю токена с записью на него сертификата и при синхронизации токена, в случае отсутствия сертификата на токене или истечении срока его действия. Содержит номер и дату формирования акта, данные по токену на который производится запись сертификата, данные по записываемому сертификату, включая УЦ и срок действия сертификата, и персональные данные пользователя, которому выдается токен с сертификатом.
Прием-передача токена в эксплуатацию	Формируется при выдаче токена пользователю (для безопасного входа по паролю, для входа по управляемому/стороннему сертификату, для учета). Содержит номер и дату формирования акта, данные по передаваемому токену и персональные данные пользователя, которому выдается токен.
Удаление сертификата с токена	Формируется при выдаче токена пользователю, при этом на токене уже имеется сертификат и его необходимо удалить, при синхронизации, в случае истечения срока действия сертификата, имеющегося на токене: удаляется истекший сертификат. Содержит номер и дату формирования акта, данные по токену с которого удаляется сертификат, данные по удаляемому сертификату, включая УЦ и срок действия сертификата, и персональные данные пользователя, которому был выпущен удаляемый сертификат.
Уничтожение токена	Формируется при удалении токена из системы. Содержит номер и дату формирования акта, данные по удаляемому токену.

При необходимости, предустановленные шаблоны можно изменить или полностью заменить созданными собственноручно.

Для изменения шаблона скачайте шаблон, который необходимо изменить по кнопке Скачать (рисунок 8.14).

Откройте сохраненный шаблон в любом доступном редакторе, поддерживающем формат ***rtf***, например, Microsoft Word 2013 (рисунок 8.15).

Акт №
уничтожения НКИ

Настоящий акт составил

ФИО Сотрудника ОИТ

ФИО Сотрудника СКЗ
о том, что сотрудник ОИТ уничтожил носитель ключевой информации

Сотрудник СКЗ

ФИО Сотрудника СКЗ

Сотрудник ОИТ

ФИО Сотрудника ИТ

Рисунок 8.15 – Изменение шаблона в редакторе

Для отображения переменных-закладок, имеющихся в шаблоне, перейдите в меню ***Файл*** → ***Параметры*** → ***Дополнительно*** и установите флаг ***Показывать закладки***.

Для добавления или изменения переменных-закладок перейдите в меню ***Вставка*** → ***Ссылки*** → ***Закладка*** и внесите необходимые изменения (рисунок 8.16).

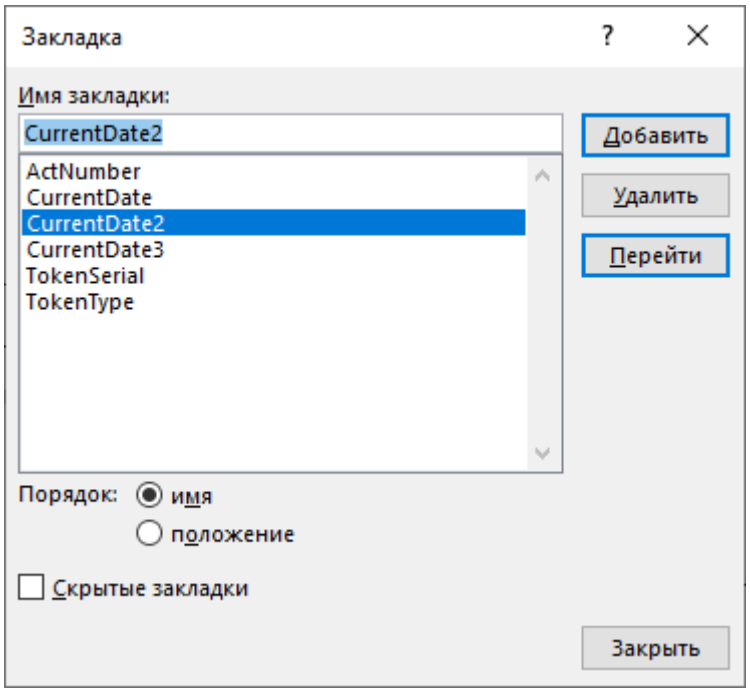
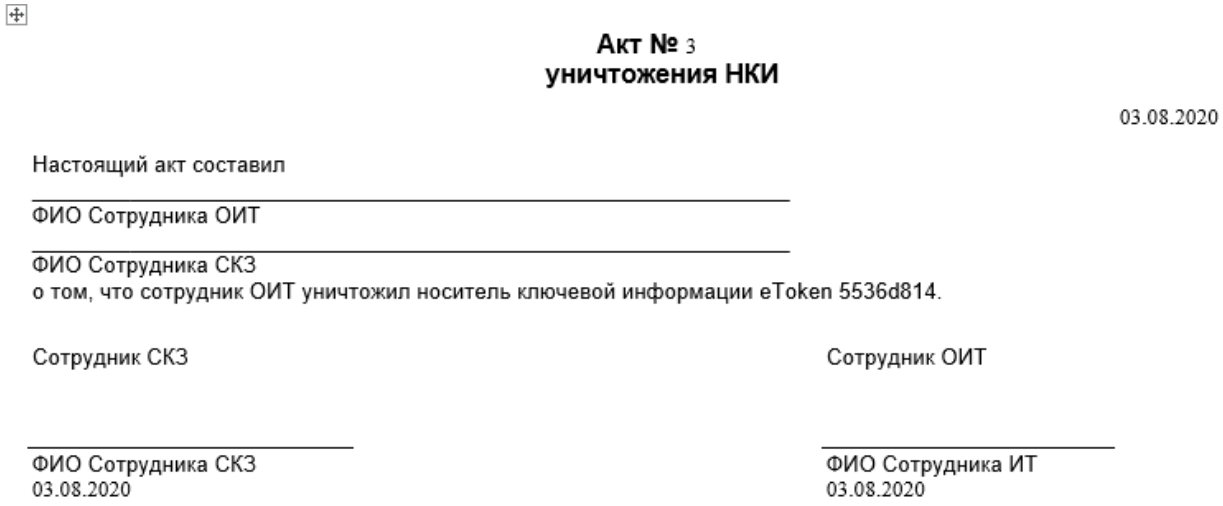


Рисунок 8.16 – Список переменных-закладок в шаблоне

Список переменных-закладок, которые можно использовать в шаблонах, представлен в таблице 8.2.

При обработке шаблона переменные-закладки будут заменены на фактические данные

(рисунок 8.17).



Акт № 3
уничтожения НКИ

03.08.2020

Настоящий акт составил

ФИО Сотрудника ОИТ

ФИО Сотрудника СКЗ
о том, что сотрудник ОИТ уничтожил носитель ключевой информации eToken 5536d814.

Сотрудник СКЗ

ФИО Сотрудника СКЗ
03.08.2020

Сотрудник ОИТ

ФИО Сотрудника ИТ
03.08.2020

Рисунок 8.17 – Отображение переменных-закладок в актах

При этом необходимо учитывать, что механизм обработки шаблонов позволяет многократно использовать одно определенное значение для закладки, которая должна повторяться в тексте, например:

Name, Name2, Name3, ..., NameN

где ***Name*** – это наименование переменной-закладки,

числа ***"2", "3", …, "N"*** – определенный индекс закладки (в качестве индекса может использоваться любое положительное число).

Таблица 8.2 – Используемые переменные-закладки

Переменная-закладка	**Пояснение**
ActNumber	Номер акта
CurrentDate	Дата акта
TokenType	Тип носителя ключевой информации (токена)
TokenSerial	Серийный номер носителя ключевой информации (токена)
TokenInventory	Инвентарный номер носителя ключевой информации (токена)
UserLogin	Наименование учетной записи сотрудника
UserFullName	ФИО сотрудника
UserFullNameOrLogin	ФИО сотрудника или, при отсутствии данных в поле, наименование учетной записи сотрудника
CertSerial	Серийный номер сертификата
CertCA	Удостоверяющий центр, выдавший сертификат
CertValidFrom	Дата начала действия сертификата
CertValidTo	Дата окончания действия сертификата

InitiatorLogin	Наименование учетной записи администратора при запуске консоли и подключении к серверу
InitiatorFullName	ФИО администратора при запуске консоли и подключении к серверу
InitiatorFullNameOrLogin	ФИО администратора или, при отсутствии данных в поле, наименование учетной записи администратора

В качестве закладок можно использовать только курсор. Помещать внутрь закладки символы, слова, ячейки таблиц и прочие конструкции запрещено!

Шаблон для формирования актов должен быть подготовлен только в формате ***rtf***.

После внесения всех необходимых изменений в файл шаблона, сохраните его.

Во вкладке ***Настройки*** в разделе ***«Шаблоны актов»*** выберите тип шаблона, который требуется заменить и нажмите кнопку 

.

При выполнении операций с токеном, акты, соответствующие типу шаблона, будут сформированы по измененному шаблону.

Создание собственного шаблона, отличного от предустановленного в системе, выполняется аналогичным образом: создается файл шаблона в формате ***rtf*** в любом доступном редакторе, вносятся необходимые переменные-закладки, перечисленные в таблице 8.2, с учетом перечисленных ограничений, и выполняется замена файла шаблона.

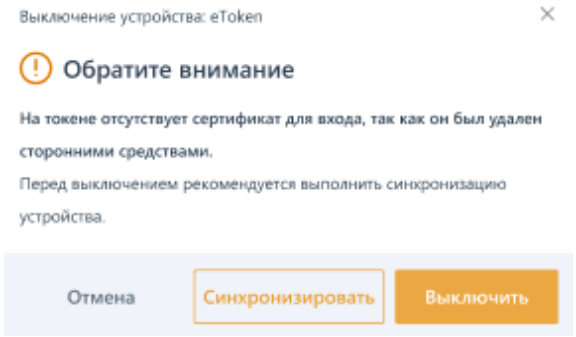
Для возврата шаблона к первоначальному виду, предустановленному в системе, перейдите в строку с требуемым типом шаблона и нажмите кнопку 

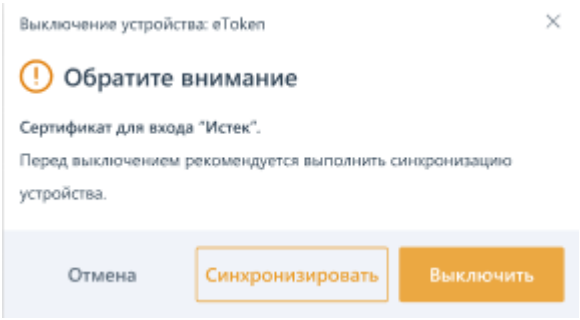
.

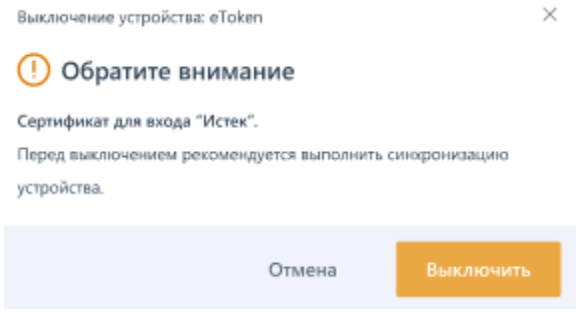
Приложение 1

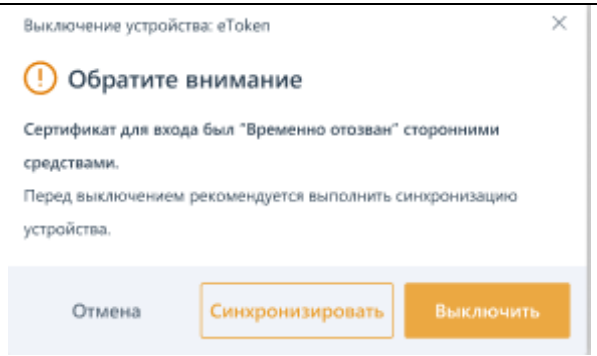
Описание возможных алгоритмов синхронизации токенов

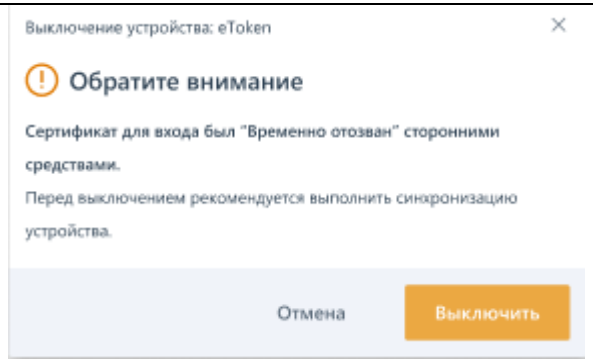
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
Используется	Выключить токен	На токене нет сертификата для входа (удален внешними средствами)	Если токен подключен к компьютеру, при выполнении операции выключения появится сообщение об отсутствии сертификата для входа на токене с рекомендацией выполнения синхронизации перед выключением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция выключения выполняется без дополнительных сообщений. 2. При выборе выключения (кнопка ***Выключить***): - токен выключается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения прерывается, токен остается в состоянии «Используется».

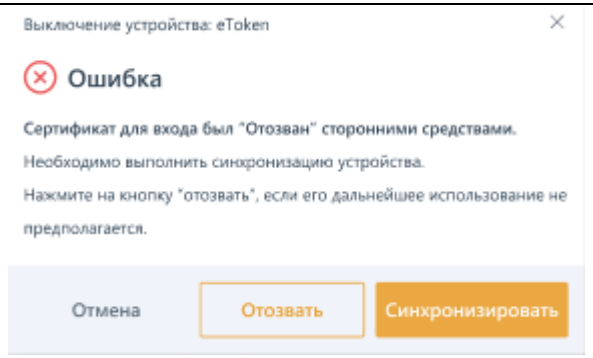
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			 Если токен не подключен к компьютеру, операция выключения выполняется в автоматическом режиме без дополнительных сообщений: - токен выключается; - сертификат временно отзывается.
		На токене истек сертификат для входа	Если токен подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа истек с рекомендацией выполнения синхронизации перед выключением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция выключения выполняется без дополнительных сообщений. 2. При выборе выключения (кнопка ***Выключить***): - токен выключается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения

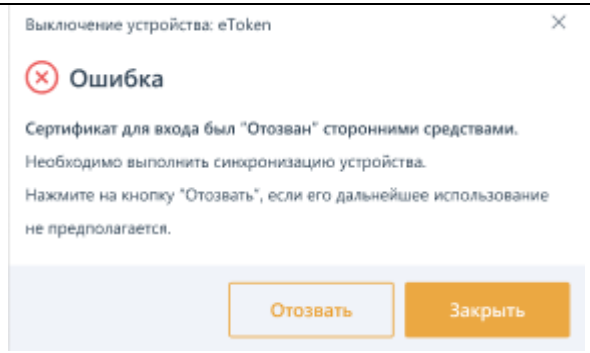
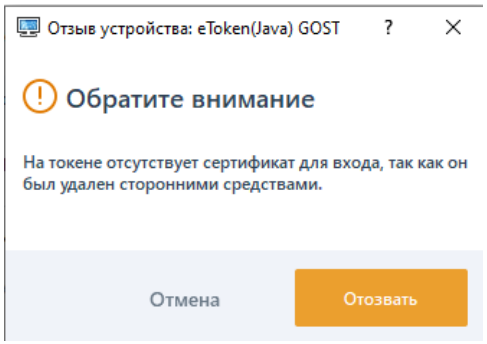
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			прерывается, токен остается в состоянии «Используется».  Если токен не подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа истек, при этом доступна только операция выключения (синхронизация возможна только для подключенных устройств). 1. При выборе выключения (кнопка ***Выключить***): - токен выключается; - сертификат временно отзывается. 2. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения прерывается, токен остается в состоянии «Используется».

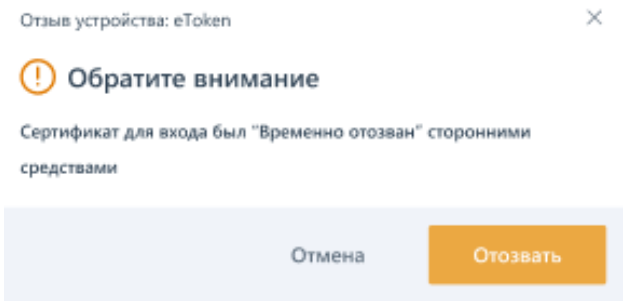
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			
		На токене сертификат для входа отозван (временно)	Если токен подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа временно отозван с рекомендацией выполнения синхронизации перед выключением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выполняется изменение статуса сертификата и сертификат возвращается из отзыва; - после синхронизации операция выключения выполняется без дополнительных сообщений. 2. При выборе выключения (кнопка ***Выключить***): - токен выключается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения прерывается, токен остается в состоянии «Используется».

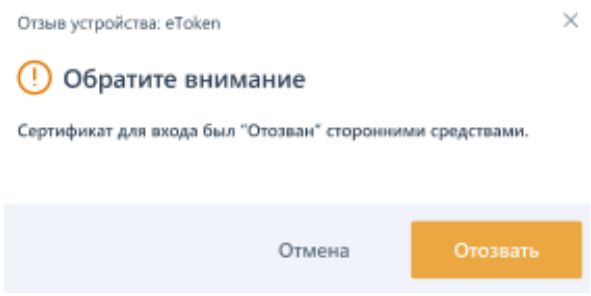
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			 Если токен не подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа временно отозван, при этом доступна только операция выключения (синхронизация возможна только для подключенных устройств). 1. При выборе выключения (кнопка ***Выключить***): - токен выключается; - сертификат временно отзывается. 2. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения прерывается, токен остается в состоянии «Используется».

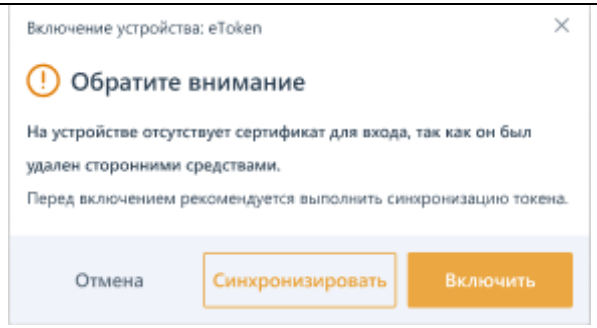
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			
		На токене сертификат для входа отозван (постоянно)	Если токен подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа отозван сторонними средствами, необходимо выполнить синхронизацию перед выключением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция выключения выполняется без дополнительных сообщений. 2. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция выключения прерывается, токен остается в состоянии «Используется».

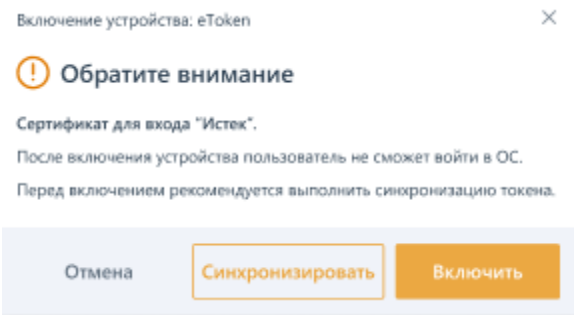
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			 Если токен не подключен к компьютеру, при выполнении операции выключения появится сообщение о том, что сертификат для входа отозван сторонними средствами, при этом доступна только операция отзыва (синхронизация возможна только для подключенных устройств). 1. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - сертификат остается в состоянии «Отозван (постоянно)». 2. При отказе от выполнения действий (кнопка ***Закрыть***), операция выключения прерывается, токен остается в состоянии «Используется».

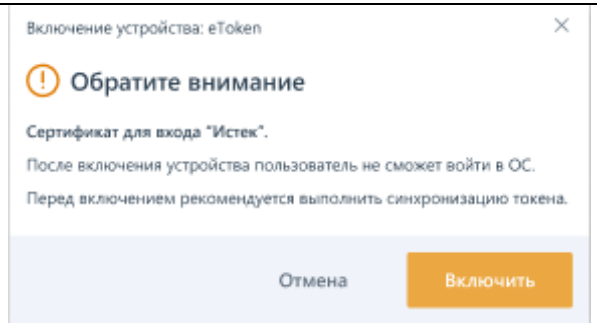
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			
	Отозвать токен	На токене нет сертификата для входа (удален внешними средствами)	Если токен подключен к компьютеру, при выполнении операции отзыва появится сообщение о том, что сертификат для входа удален сторонними средствами. 1. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - сертификата на токене удаляется. 2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Используется».  Если токен не подключен к компьютеру, операция отзыва выполняется в

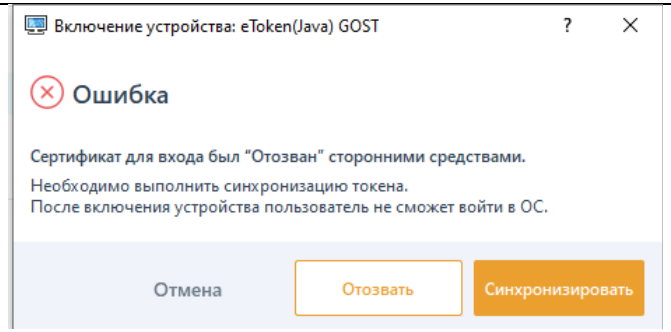
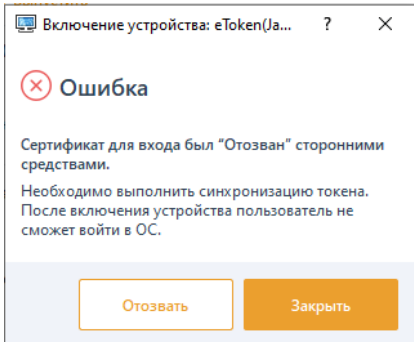
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			автоматическом режиме без дополнительных сообщений: - токен отзывается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется.
		На токене сертификат для входа отозван (временно)	При выполнении операции отзыва появится сообщение о том, что сертификат для входа временно отозван. 1. При выборе операции отзыва (кнопка ***Отозвать***): - токен переходит в состояние «Отозван»; - сертификат отзывается (постоянно). 2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Используется». 
		На токене сертификат для входа отозван (постоянно)	При выполнении операции отзыва появится сообщение о том, что сертификат для входа уже отозван. 1. При выборе операции отзыва (кнопка ***Отозвать***): - токен переходит в состояние «Отозван»; - сертификат остается в состоянии «Отозван (постоянно)».

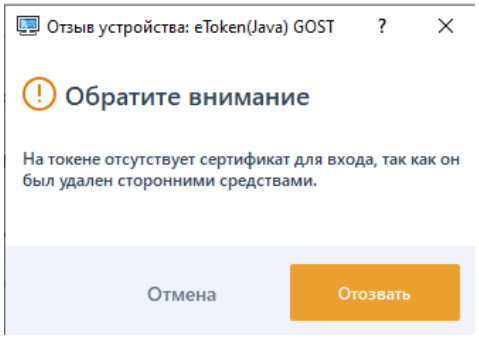
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Используется». 
Выключен	Включить токен	На токене нет сертификата для входа (удален внешними средствами)	Если токен подключен к компьютеру, при выполнении операции включения появится сообщение об отсутствии сертификата для входа на токене с рекомендацией выполнения синхронизации перед включением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция включения выполняется без дополнительных сообщений. 2. При выборе включения (кнопка ***Включить***): - токен включается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция включения прерывается, токен остается в состоянии «Выключен».

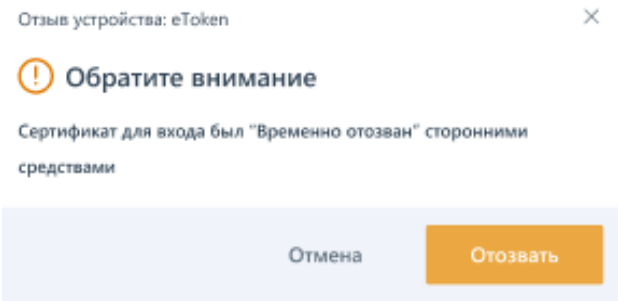
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			 Если токен не подключен к компьютеру, операция включения выполняется в автоматическом режиме без дополнительных сообщений: - токен включается; - сертификат переходит в состояние «Действующий».
		На токене истек сертификат для входа	Если токен подключен к компьютеру, при выполнении операции включения появится сообщение о том, что сертификат для входа истек (после включения устройства пользователь не сможет войти в ОС) с рекомендацией выполнения синхронизации перед включением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция включения выполняется без дополнительных сообщений. 2. При выборе включения (кнопка ***Включить***): - токен включается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется;

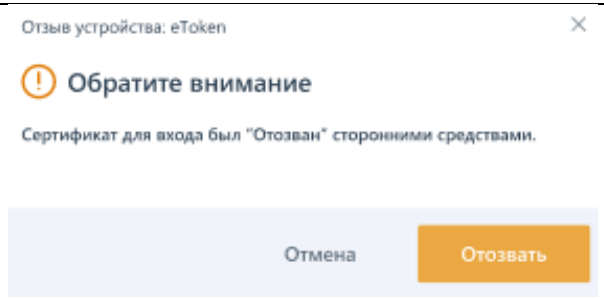
Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			- сертификат переходит в состояние «Истек». 3. При отказе от выполнения действий (кнопка ***Отмена***), операция включения прерывается, токен остается в состоянии «Выключен».  Если токен не подключен к компьютеру, при выполнении операции включения появится сообщение о том, что сертификат для входа истек (после включения устройства пользователь не сможет войти в ОС), при этом доступна только операция включения (синхронизация возможна только для подключенных устройств). 1. При выборе включения (кнопка ***Включить***): - токен включается; - сертификат переходит в состояние «Действующий». 2. При отказе от выполнения действий (кнопка ***Отмена***), операция включения прерывается, токен остается в состоянии «Выключен».

Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			
		На токене сертификат для входа отозван (постоянно)	Если токен подключен к компьютеру, при выполнении операции включения появится сообщение о том, что сертификат для входа отозван сторонними средствами (после включения устройства пользователь не сможет войти в ОС), необходимо выполнить синхронизацию перед включением токена. 1. При выборе синхронизации (кнопка ***Синхронизировать***): - выпускается новый сертификат и записывается на токен; - после синхронизации операция включения выполняется без дополнительных сообщений. 2. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется. 3. При отказе от выполнения действий (кнопка ***Отмена***), операция включения прерывается, токен остается в состоянии «Выключен».

Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			 Если токен не подключен к компьютеру, при выполнении операции включения появится сообщение о том, что сертификат для входа отозван сторонними средствами, при этом доступна только операция отзыва (синхронизация возможна только для подключенных устройств). 1. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - сертификат остается в состоянии «Отозван (постоянно)». 2. При отказе от выполнения действий (кнопка ***Закрыть***), операция включения прерывается, токен остается в состоянии «Выключен». 

Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
	Отозвать токен	На токене нет сертификата для входа (удален внешними средствами)	Если токен подключен к компьютеру, при выполнении операции отзыва появится сообщение о том, что сертификат для входа удален сторонними средствами. 1. При выборе отзыва сертификата (кнопка ***Отозвать***): - токен отзывается; - сертификат на токене удаляется. 2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Выключен».  Если токен не подключен к компьютеру, операция отзыва выполняется в автоматическом режиме без дополнительных сообщений: - токен отзывается; - синхронизация с фактическим состоянием сертификата на токене не осуществляется.

Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
		На токене сертификат для входа отозван (временно)	При выполнении операции отзыва появится сообщение о том, что сертификат для входа временно отозван. 1. При выборе операции отзыва (кнопка ***Отозвать***): - токен переходит в состояние «Отозван»; - сертификат отзывается (постоянно). 2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Выключен». 
		На токене сертификат для входа отозван (постоянно)	При выполнении операции отзыва появится сообщение о том, что сертификат для входа уже отозван. 1. При выборе операции отзыва (кнопка ***Отозвать***): - токен переходит в состояние «Отозван»; - сертификат остается в состоянии «Отозван (постоянно)». 2. При отказе от выполнения действий (кнопка ***Отмена***), операция отзыва прерывается, токен остается в состоянии «Выключен».

Состояние токена в ЖЦТ	Выполняемая операция	Описание алгоритма синхронизации	Состояние токена после выполнения операции
			

Перечень сокращений

PIN	–	Personal Identification Number (личный идентификационный номер)
PKI	–	Public Key Infrastructure (инфраструктура открытых ключей)
АРМ	–	Автоматизированное рабочее место
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
СЗИ	–	Средство защиты информации
УЦ	–	Удостоверяющий центр