ГАЗИНФОРМСЕРВИС

Управление токенами в серверной консоли БХС 2.0.

1. Введение

Все токены в БХС можно разделить на две категории: отчуждаемые токены и считыватели типа реестра, они же виртуальные токены. К отчуждаемым токенам можно отнести флэш-накопители и защищённые токены всех типов, такие как etoken, jacarta, rutoken и другие (см. руководство администратора БХС). Данный тип токенов в БХС 2.0 используются для построения системы двухфакторной аутентификации. Как показала практика, использование отчуждаемых токенов для развертывания клиентов БХС нецелесообразно. Настройка отчуждаемых приводила к существенному осложнению процесса установки, увеличению временных и эксплуатационных затрат на развёртывание СЗИ. В этой связи в БХС 2.0 были введены так называемые виртуальные токены. Это области реестра, в которые в зашифрованном виде записывается информация, аналогичная, той, что содержится на отчуждаемых токенах. При этом такие считыватели имеют ряд преимуществ перед отчуждаемыми токенами. Виртуальные считыватели всегда присутствуют в машине при ее корректном запуске, следовательно, нет риска утраты и проблем с драйверами и аппаратной частью. Количество пользователей на одном считывателе, как и количество самих считывателей ограниченно только размерами жесткого диск, в то время как для отчуждаемого токена такие ограничения составляют около 100 пользователей (в зависимости от модели токена). В БХС 2.0 реализована возможность централизованного управления виртуальными токенами клиентов с помощью серверной консоли БХС. Так как в БХС 2.0 клиенты могут управляется с сервера до входа пользователя, то в случае проблем с отчуждаемым токеном пользователя (по причине его временной утраты, например) администратор безопасности может оперативно создать для пользователя временный виртуальный считыватель, обеспечив возможность входа на станцию до момента решения проблемы с отчуждаемым токеном.

2. Администрирование токенов в серверной консоли БХС 2.0

Серверная консоль БХС 2.0 предоставляет администратору безопасности широкие возможности по управлению и администрированию токенов сети безопасности БХС. Для управления и получения информации о токенах сети безопасности БХС используется окно «Токены» консоли администрирования БХС. Окно по умолчанию расположено под окном «Настройки машины» как на рисунке 1. Окно токены может быть временно закрыто для удобства управления другими настройками БХС, включить его отображение можно в меню «Вид», пункт «Список токенов».

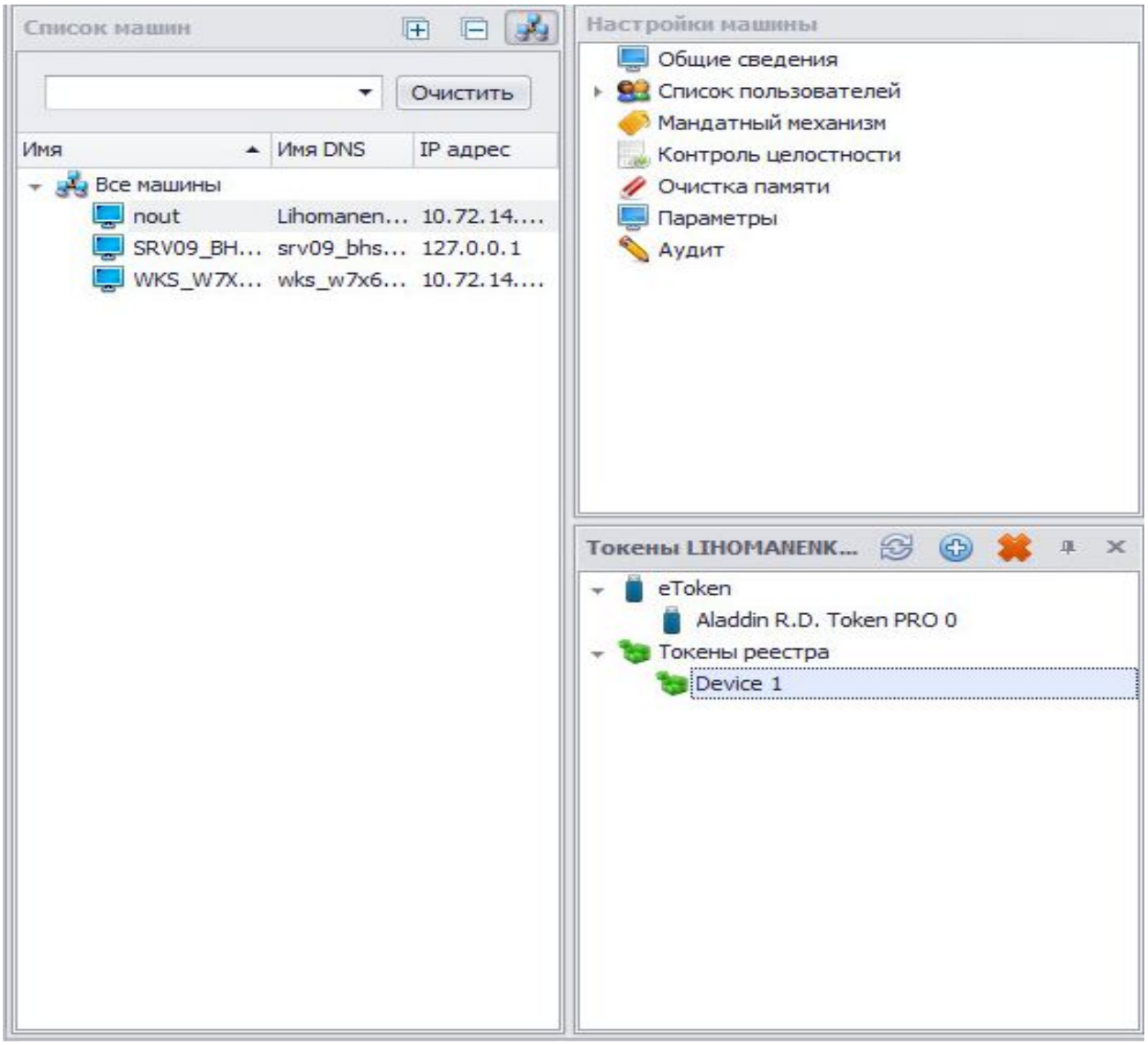

Рисунок 1: Окно администрирования токенов клиента.

В окне «Токены» отображается список всех токенов, которые на данный момент имеются на выбранном в списке машин клиенте. Все токены, отображаемые в данном окне, доступны к администрированию. С помощью данного окна администратор безопасности имеет возможность просматривать подключенные к клиенту токены всех типов, удалить или добавить виртуальный считыватель для выбранного клиента, а также войти на токен и получить доступ к меню управления токеном. Обращаем ваше внимание, что для получения корректного списка токенов, подключенных непосредственно к серверу БХС, необходимо в окне список машин выбрать пункт «Все машины». Для получения доступа к меню управления токеном необходимо два раза щелкнуть правой клавишей мыши на токене, войти на который вы хотите, и появившемся модальном окне ввести его пинкод (смотри рисунок 2)

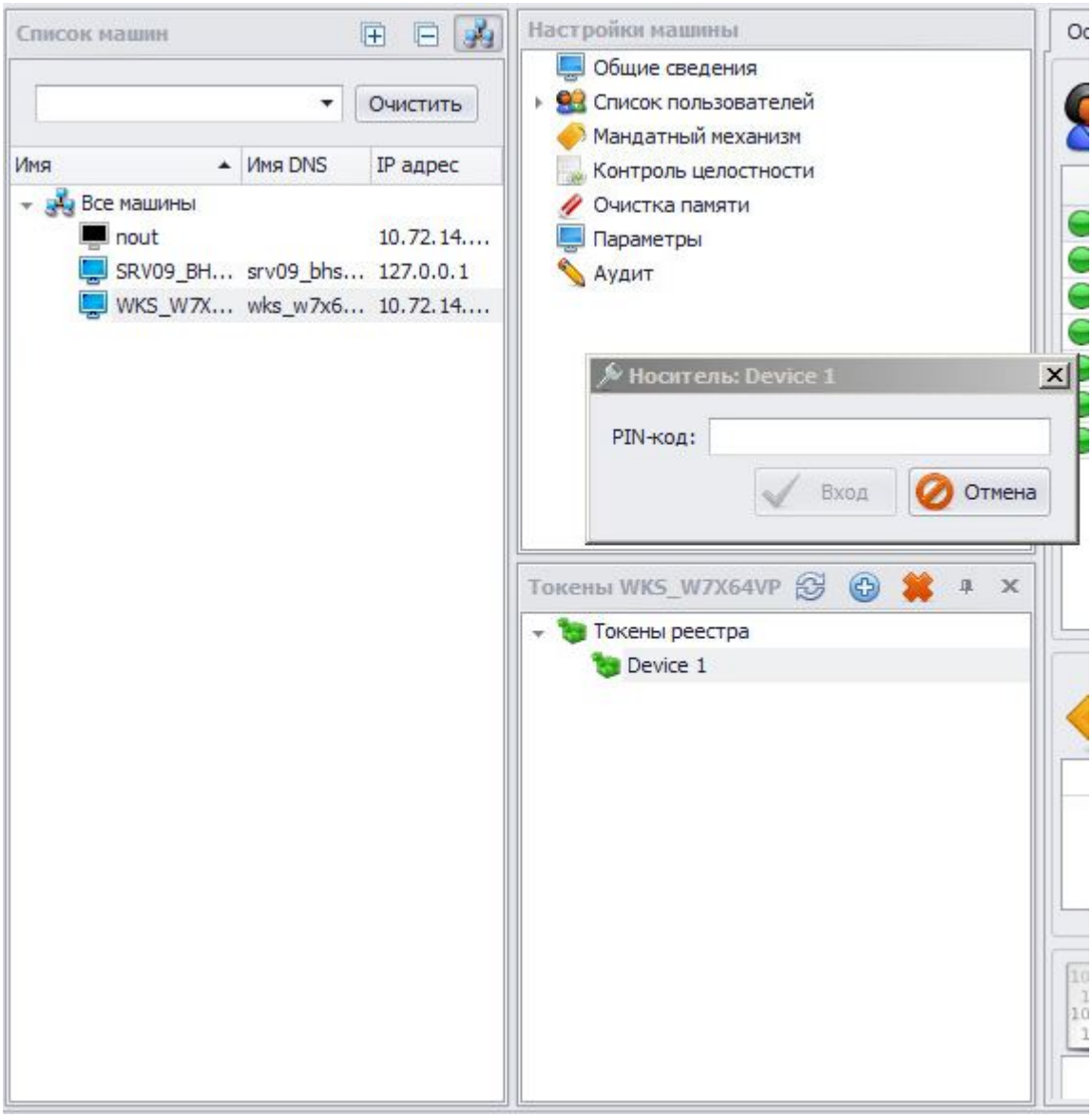

Рисунок 2: Ввод пинкода для входа на виртуальный считыватель Device 1

После корректного ввода пинкода токена в правой части консоли откроется окно управления токеном (смотри рисунок 3) В этом окне администратор имеет возможность произвести следующие действия: просматривать и редактировать список заведенных на токене пользователей и рабочих станций, произвести экспорт и импорт ключевого контейнера токена в зашифрованный файл, инициализировать токен, ограничить время жизни токена или заблокировать его, а также сменить пинкод данного токена.

Экспорт и импорт ключевого контейнера токена – новый функционал, который появился только в БХС 2.0. Он позволяет администратору безопасности с помощью кнопки «Экспорт» сохранить копию любого токена БХС в зашифрованный файл. Из такого файла содержимое токена с помощью кнопки «Импорт» можно записать на любой другой отчуждаемый или виртуальный токен БХС. Данный функционал можно использовать как средство резервного копирования отчуждаемых токенов. Также с помощью этого механизма можно производить передачу содержимого токена для отладки или миграции.

Выполнение процедуры инициализации токена приведет к удалению всей информации БХС с токена. Инициализацию необходимо выполнять, когда необходимо полностью очистить контейнер БХС токена.

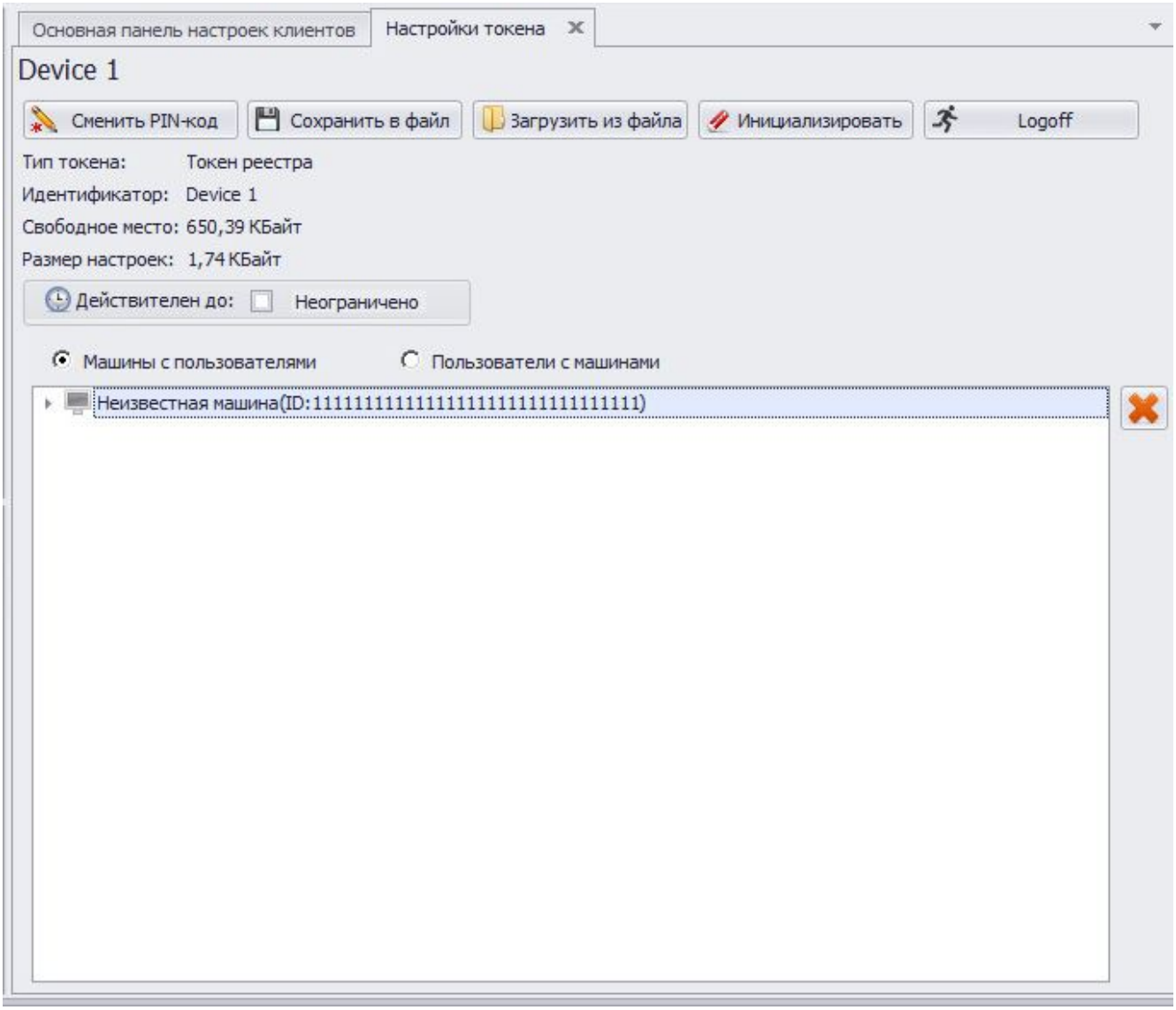

Рисунок 3: Окно управления токеном

Процедуру присвоения токена пользователю БХС осуществляется через окно «Настройки машины», пункт меню список пользователей. Щелкнув на этот пункт правой клавишей мыши вы увидите справа список пользователей данного клиента. Сверху же откроется меню редактирования пользователей, где будет пункт «Управление носителями». Для присвоения токена тому или иному пользователю, необходимо выбрать данного пользователя одним щелчком левой клавиши мыши и нажать на кнопку «Управление носителями» как на рисунке 4. После этого появится модальное окно управления носителями выбранного пользователя рабочей станции. С помощью этого меню можно выполнить следующие операции: произвести добавление токена для выбранного пользователя, отвязать токен, выданный ранее, и заблокировать (разблокировать) привязанный к пользователю токен.

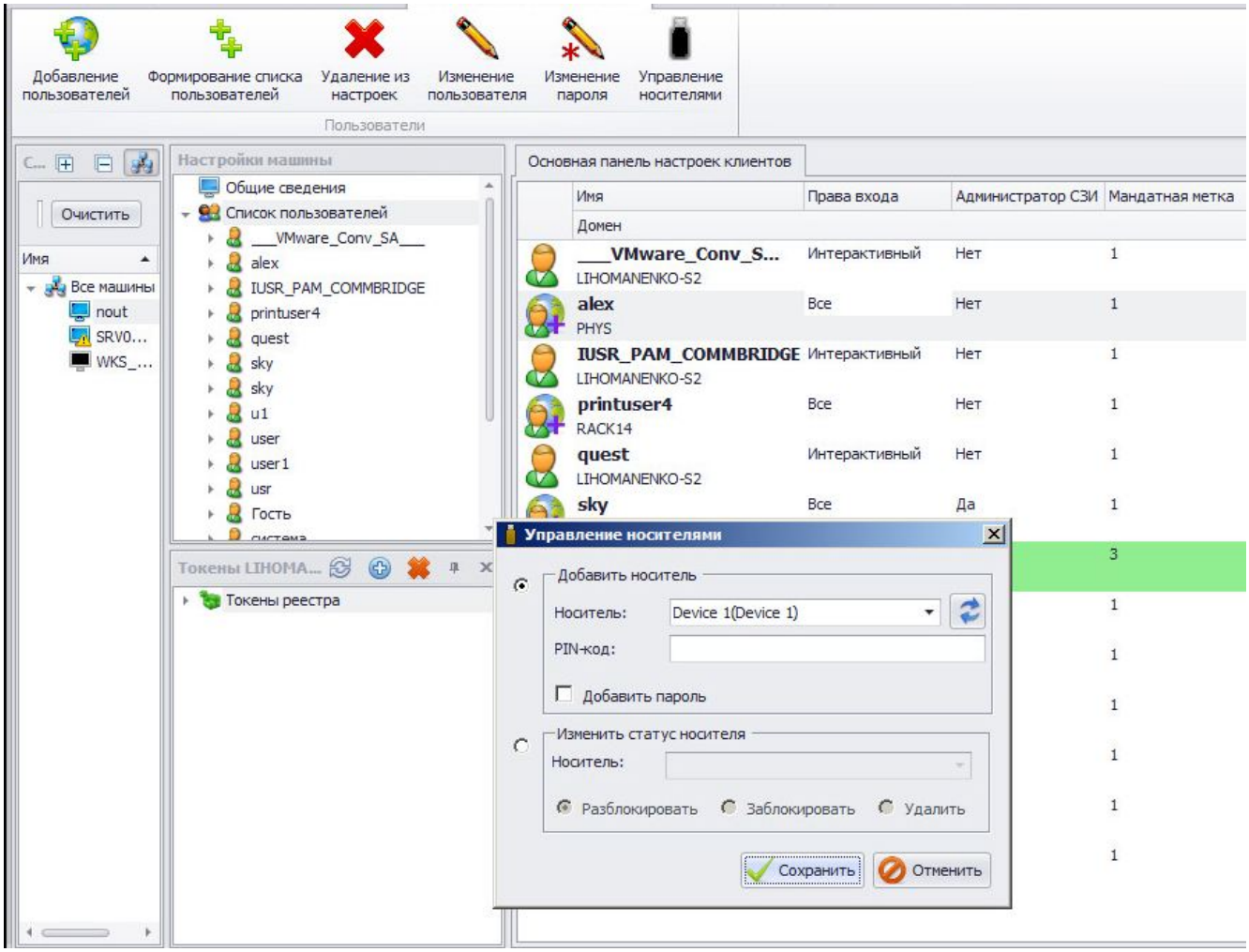

Рисунок 4: Окно управления токенами пользователя

Операция добавления токена выполняется с помощью пункта «Добавить носитель». Для добавления токена необходимо выбрать его из выпадающего списка (смотри рисунок 5), ввести в строку PIN- код его пинкод, и нажать клавишу сохранить. В результате этой процедуры выбранный токен будет добавлен для данного пользователя на выбранной рабочей станции. В выпадающем списке будут показаны как токены, подключенные к клиенту, так и токены, подключенные к серверу БХС. Последние будут помечены подписью «Сервер» (смотри рисунок 5)

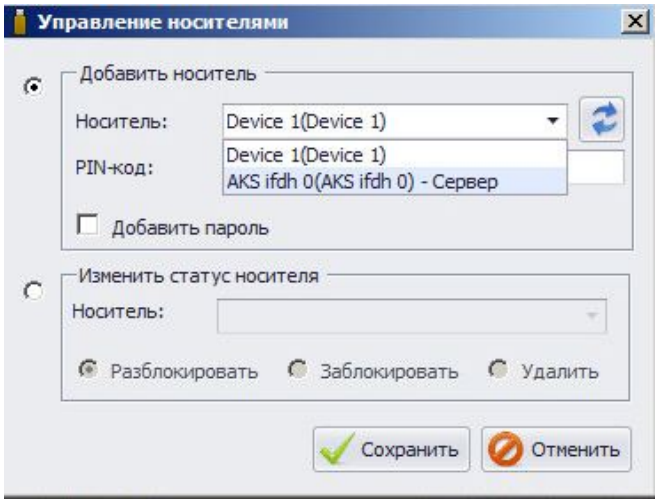

Рисунок 5: Список токенов на клиенте

Все токены в списке доступны для добавления пользователю. Отвязать токен от пользователя можно с помощью пункта меню «Удалить» в меню «Изменить статус носителя». При этом важно понимать, что эта процедура не приведет к удалению или инициализации выбранного носителя. При выполнении операции выбранный носитель будет удален из конфигурационного файла БХС для выбранного пользователя. На практике это означает, что выбранный пользователь больше не сможет осуществлять интерактивный вход с данным токеном. Функционал блокировки (разблокировки) токена работает похожим образом, с той разницей, что возможность входа пользователя с данным токеном блокируется путем внесения отметки о блокировке в конфигурационный файл БХС. Пользователь с заблокированным токеном также не сможет выполнить интерактивный вход в ОС. Операция разблокировки делает токен опять доступным для входа выбранного пользователя.

3. Практические примеры администрирования ключевых носителей в сети безопасности БХС

В данном пункте мы на практике разберем решение некоторых типичных кейсов администратора безопасности, возникающих при администрировании сети безопасности БХС с помощью консоли администрирования сервера. Кейсы будут касаться вопросов управления токенами и пользователями сети безопасности БХС.

Пример 1: Перевод пользователя рабочей станции на двухфакторную аутентификацию после установки клиента с помощью системы развертывания msi.

Исходные данные: Мы завершили развертывания БХС на ПК nout с помощью системы развертывания msi. Все пользователи данного ПК были добавлены в консоль БХС с виртуальным считывателем device1 и пинкодом по умолчанию, мягкий режим отключен.

Задача: необходимо перевести пользователя user1 домена rack14 на двухфакторную аутентификацию по etoken.

Для решения задачи необходимо в списке машин открыть компьютер nout и выбрать в окне настройки машины пункт «Список пользователей». Справа от окна настройки машины появится список пользователей машины, а в верхнем меню иконки операций по управлению пользователями и токенами (смотри рисунок 6).

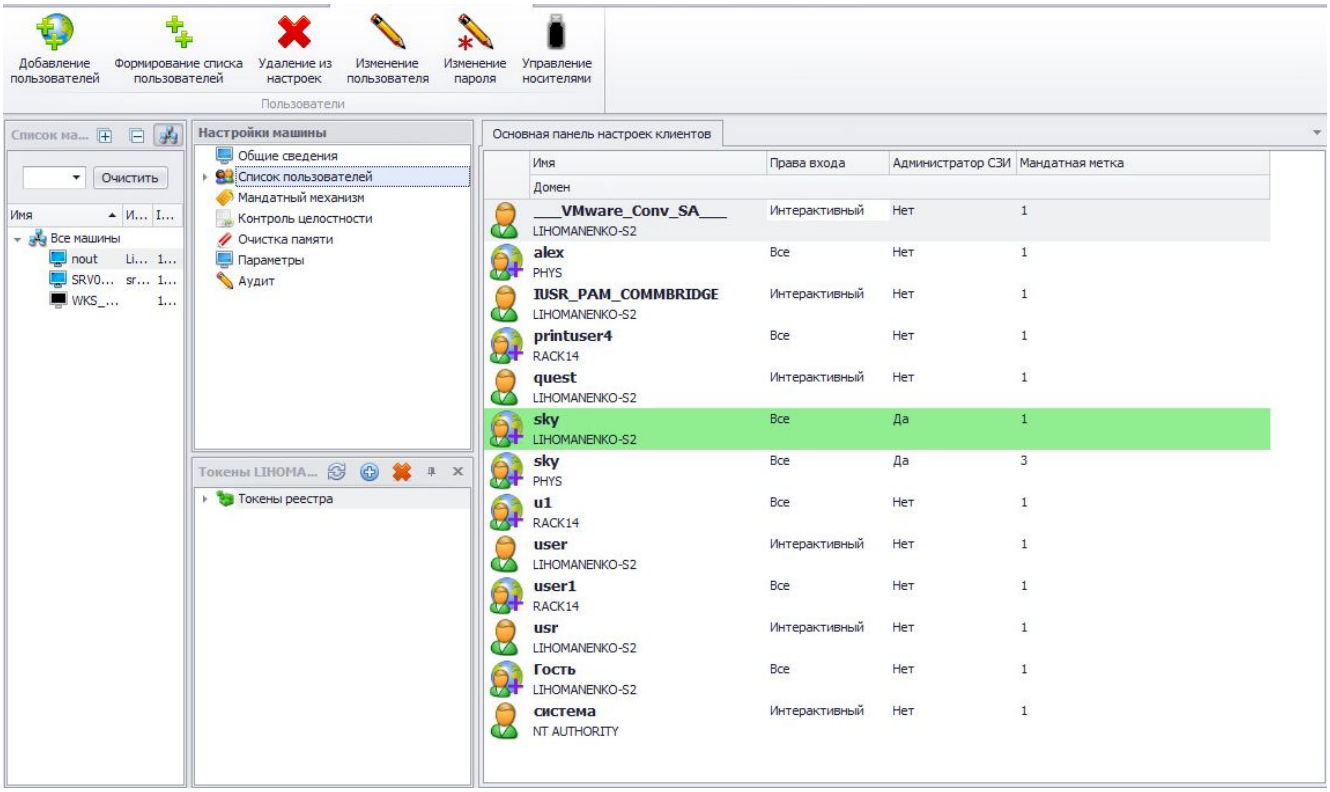

Рисунок 6: окно управления пользователями

Зеленным будет выделен пользователь, который в настоящий момент выполнил интерактивный вход на данную машину. Для начала необходимо перевести управление на пользователя user1 из задания, однократно щелкнув по его имени в списке левой клавишей мыши. После выполнения этой операции имя пользователя будет подсвечено серым цветом. Далее необходимо с помощью иконки верхнего меню управление носителями вызвать одноименное модальное окно (смотри рисунок 7).

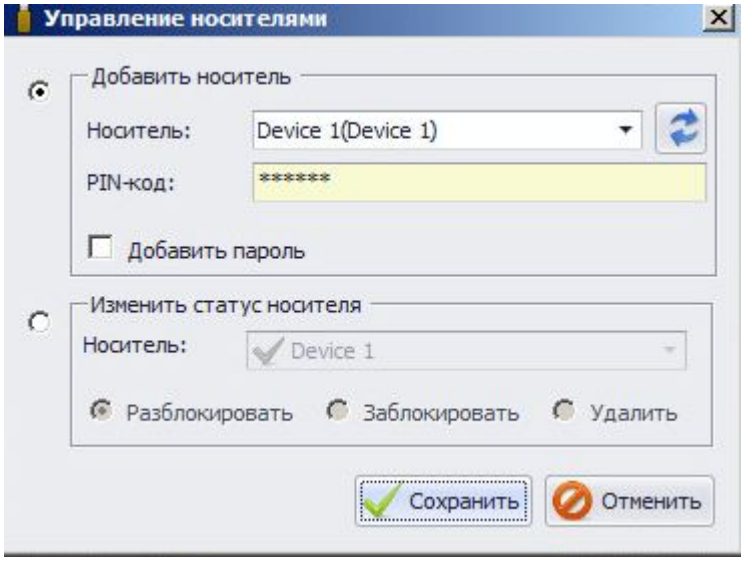

Рисунок 7: Окно управления носителями

В окне управления носителями необходимо выбрать опцию «Изменить статус носителя». В выпадающем меню справа появится список носителей, привязанных к данному пользователю. В нашем случае там будет носитель device1, выданный пользователю системой развертывания msi при установке клиента БХС (смотри рисунок 8).

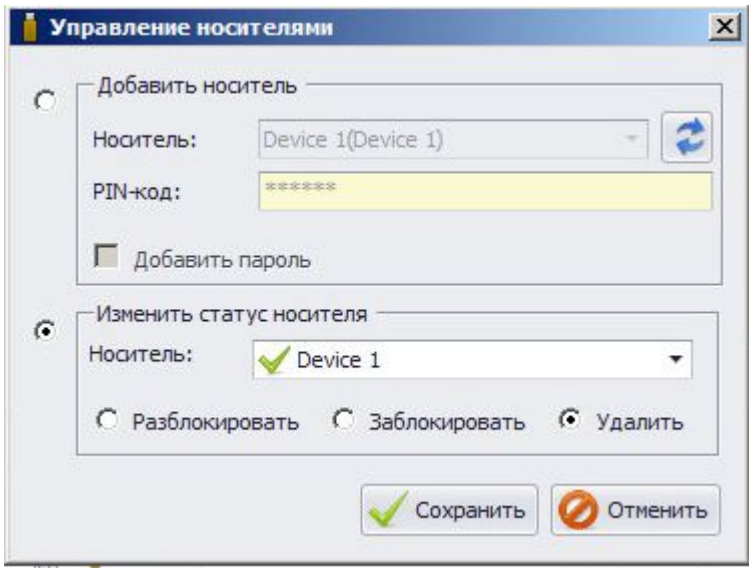

Рисунок 8: Удаление носителя device1 из списка доступных для двухфакторной аутентификации пользователя user1

После нажатия кнопки «Сохранить» носитель device1 будет недоступен для входа в систему с ученой записью user1 из домена Rack14. Далее необходимо добавить пользователю отчуждаемый носитель etoken. Для этого необходимо повторно вызвать меню управления носителями и выбрать опцию добавить носитель. Далее необходимо подключить носитель либо к серверу БХС, либо к ПК nout. После подключения токена необходимо нажать клавишу обновить (кнопка с с двумя противоположными стрелками). После обновление подключенный носитель появится в выпадающем списке доступных для добавления носителей (смотри рисунок 9)

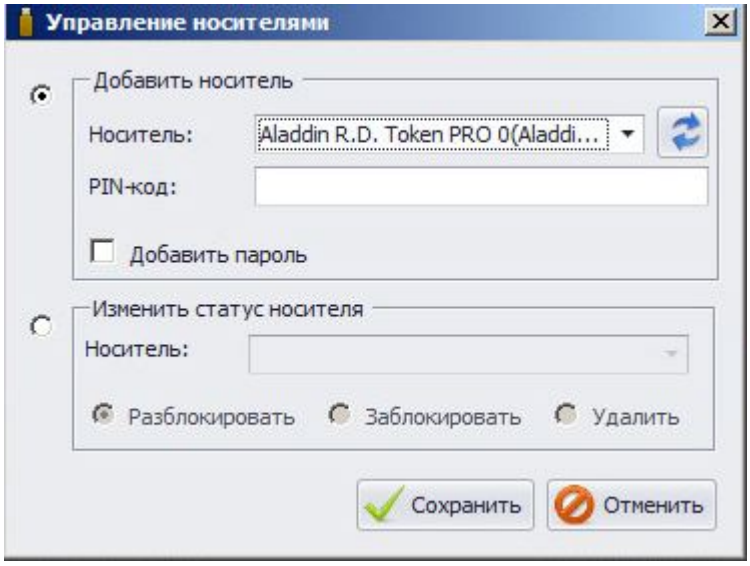

Рисунок 9: Добавление токена пользователю.

Для добавления токена пользователю user1 необходимо ввести пинкод токена и нажать клавишу «Сохранить». После успешного выполнения всех этих процедур необходимо произвести настроек в серверной консоли. С этого момента пользователю будет доступна

двухфакторная аутентификация, при этом вход с помощью носителя device1 станет недоступен.