ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Центр-Т»

(Версия 1.3.2)

Руководство по эксплуатации клиентских устройств

37222406.26.20.40.140.042 34

Листов 49

Москва
2024

АННОТАЦИЯ

Настоящий документ является руководством по управлению клиентскими устройствами из состава программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Центр-Т» (далее – ПАК «Центр-Т», Комплекс) – носителями ПО Клиента – и предназначен для должностных лиц, выполняющих роли Администратора безопасности информации клиентских устройств (далее – Администратор БИ), Администратора клиентских устройств (далее – Администратор) и Пользователей клиентских устройств (далее также – Пользователь).

В документе конкретизируются задачи и функции должностных лиц организации (предприятия, фирмы), планирующих и организующих защиту информации в системах и средствах информатизации на базе средств вычислительной техники (СВТ) с применением Комплекса, а также использующих Комплекс по прямому назначению – для получения образа ПО ТС по сети.

Для эффективного использования механизмов Комплекса рекомендуется принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных мер Комплекса должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

ПАК «Центр-Т» представляет собой комплекс программных и аппаратных средств, позволяющий осуществлять хранение и сетевую загрузку программного обеспечения (ПО) терминальных станций (ТС), которые используются в системе терминального доступа, с возможностью обработки информации ограниченного доступа.

В состав аппаратных средств ПАК «Центр-Т» входят следующие компоненты:

- носитель ПО Клиента (далее – клиентское устройство);
- носитель ПО Сервера хранения и сетевой загрузки (СХСЗ).

Носители поставляются с уже записанными образом начальной загрузки (ОНЗ) и лицензией.

Схема работы выглядит следующим образом:

1) с носителя ПО СХСЗ стартует ПО СХСЗ. На момент начала эксплуатации оно содержит образы операционной системы (ОС) Linux с необходимым ПО для соединения с терминальным сервером;

2) с носителя ПО Клиента стартует образ начальной загрузки, также реализованный на основе ОС Linux. Далее на СХСЗ посылается запрос на получение назначенных образов ПО ТС (Пользователю может быть назначено несколько образов ПО ТС);

3) СХСЗ обрабатывает запрос и выдает клиенту нужный образ (образы) ПО ТС;

4) клиентское устройство принимает образ (образы) по сети и проверяет его. Если проверка образа завершается успешно, то он загружается;

5) ПО, запущенное из полученного образа, инициирует соединение с терминальным сервером и осуществляет идентификацию Пользователя на сервере.

Функции ПО Клиента разделены между тремя ролями: Администратор, Администратор БИ и Пользователь. Функции Администратора и Администратора БИ клиентских устройств могут быть возложены на одно должностное лицо, если это предусмотрено регламентирующими документами эксплуатирующей организации.

Для эффективного применения ПАК «Центр-Т» и поддержания требуемого уровня защищенности СВТ необходимы:

- разработка и ведение учетной и объектовой документации (инструкции администраторов и пользователей, журнал учета идентификаторов и др.). Все документы должны быть согласованы, утверждены у руководства и доведены до сотрудников. Это необходимо для того, чтобы План защиты информации организации (предприятия, фирмы и т.д.) и действия службы БИ получили юридическую основу;

- оформление приема в эксплуатацию ПАК «Центр-Т» актом в установленном порядке, указание в формуляре на Комплекс соответствующей информации.

1 Объем работы ролей клиентских устройств

Основными процедурами, выполняемыми ролями клиентских устройств, являются:

- планирование применения клиентских устройств;
- запись в клиентские устройства образа начальной загрузки (при необходимости);
- установка PIN-кодов Администратора и Администратора БИ;
- копирование файла лицензии на клиентское устройство (при необходимости);
- установка сетевых настроек Клиента;
- установка сетевых настроек для связи с СХСЗ;
- установка настроек даты и времени Клиента;
- резервирование и восстановление локальных настроек Клиента;
- работа в рамках терминальной сессии;
- смена PIN-кода Администратора;
- смена PIN-кода Администратора БИ;
- просмотр событий безопасности;
- изменение разрешения экрана;
- настройка тайм-аута гашения экрана;
- настройка аудиоустройств;
- настройка принтеров;
- просмотр сетевых настроек Клиента;
- проверка работоспособности сети.

Планирование применения клиентских устройств осуществляется администраторами клиентских устройств, порядок планирования описан в разделе 2.

Администратор клиентских устройств производит:

- запись ОНЗ;
- установку PIN-кода Администратора;
- установку сетевых настроек Клиента;
- настройку даты и времени;
- смену PIN-кода Администратора.

Администратор БИ клиентских устройств производит:

- установку PIN-кода Администратора БИ;
- установку сетевых настроек для связи с СХСЗ;
- копирование файла лицензии на клиентское устройство (при необходимости);
- резервирование и восстановление локальных настроек Клиента;
- смену PIN-кода Администратора БИ;
- просмотр событий безопасности;
- управление отладочным режимом.

Пользователь клиентского устройства осуществляет:

- работу в рамках терминальной сессии;

- изменение разрешения экрана;
- настройку тайм-аута гашения экрана;
- настройку аудиоустройств;
- настройку принтеров;
- просмотр сетевых настроек Клиента;
- проверку работоспособности сети.

2 Планирование применения клиентских устройств

Планирование применения клиентских устройств осуществляется с учетом общей политики обеспечения безопасности в организации (на предприятии, фирме и т.д.).

Для настройки и эксплуатации клиентских устройств Администратор должен получить перечень соответствующих им настроек сети (IP-адреса, маски сети, шлюз и т. д.).

Для настройки и эксплуатации клиентских устройств в соответствии с перечнем выполняемых действий Администратору БИ также необходимо предварительно получить от Администратора сервисного режима СХСЗ адрес и порт RMQ и хранилища с образами ПО ТС.

Для возможности создания любому Пользователю изолированной программной среды необходимо, чтобы общая политика обеспечения безопасности и правила разграничения доступа к ресурсам гарантировали:

– исключение возможности доступа непривилегированных Пользователей к имеющимся на СВТ инструментальным и технологическим программам, с помощью которых можно проанализировать работу средств защиты информации и предпринять попытки их «взлома» и обхода, внедрения разрушающих программных воздействий;

– исключение возможности разработки программ в защищенном контуре СВТ (системы);

– исключение возможности несанкционированной модификации и внедрения несанкционированных программ;

– жесткое ограничение круга лиц, обладающих расширенными или неограниченными полномочиями по доступу к защищаемым ресурсам.

При наличии в системе большого количества пользователей можно оптимизировать процесс инициализации клиентских устройств, производя их настройку на одном СВТ. Для обеспечения такой возможности рекомендуется использовать АРМ Эмиссии, входящее в расширенный комплект поставки ПАК «Центр-Т». Пользователи клиентских устройств могут использовать в качестве терминальной станции СВТ архитектуры x86-64 с аппаратной поддержкой виртуализации и возможностью загрузки с USB-устройств или же Защищенный терминал Центр-TrusT. В первом случае загрузка терминальной станции происходит с носителя ПО Клиента, во втором – с диска Защищенного терминала Центр-TrusT. В обоих случаях настройки, определяющие работу пользователя в ПАК «Центр-Т», хранятся на носителе ПО Клиента[1]. Одно и то же клиентское устройство может использоваться как на СВТ с архитектурой x86-64, так и совместно с Защищенным терминалом Центр-TrusT при условии назначения пользователю клиентского устройства образов с архитектурой обоих типов.

[1] Подробнее о работе пользователей клиентских устройств на Защищенном терминале Центр-TrusT – ПРИЛОЖЕНИЕ 5

3 Состав работ Администратора клиентских устройств

3.1 Общие сведения

После получения клиентского устройства Администратор должен:

1) при необходимости записать ОНЗ в клиентское устройство (см. 3.2);
2) получить доступ к ПО Клиента и установить PIN-код Администратора при первом доступе (см. 3.3);
3) установить сетевые настройки клиентского устройства (см. 3.4).

В процессе эксплуатации Комплекса Администратор может изменять свой PIN-код (см. 3.6).

Примечание: *Если в системе предусмотрено АРМ Эмиссии, часть настроек клиентских устройств может выполнять администратор АРМ Эмисси (подробнее см. Руководство по эксплуатации АРМ Эмиссии 37222406.26.20.40.140.042 92).*

3.2 Запись образа начальной загрузки

Носители ПО Клиента поставляются с уже записанным ОНЗ. Но при необходимости можно обновить образ, записав его в клиентское устройство с помощью утилиты USBWriter.exe из комплекта поставки продукта.

В текущей версии Комплекса предоставляются следующие варианты загрузчиков образов:

- client_syslinux.img - для записи на специальные носители Центр-Т с объемом памяти 4Гб;
- client_syslinux_8G.img - для записи на специальные носители Центр-Т с объемом памяти 8Гб.

3.3 Получение доступа к ПО Клиента

Для получения доступа к ПО Клиента Администратору необходимо осуществить загрузку СВТ в режиме работы с ПАК «Центр-Т». Возможны два способа загрузки:

- загрузка с носителя ПО Клиента, если в качестве СВТ используется терминал с архитектурой x86-64 и поддержкой загрузки по USB;
- загрузка с диска Защищенного терминала Центр-TrusT и подключение клиентского устройства к нему[2].

В результате загрузки ПО Клиента запускается главное окно приложения. Для доступа к функциям администрирования Администратор клиентского устройства должен перейти на вкладку «Администратор».

Если загрузка ПО сервисного режима работы выполняется впервые, необходимо пройти обязательную процедуру установки PIN-кода Администратора, который будет использоваться в дальнейшем для доступа к функциям администрирования, соответствующим этой роли (рисунок 1).

[2] Подробнее о работе пользователей клиентских устройств на Защищенном терминале Центр-TrusT - ПРИЛОЖЕНИЕ 5

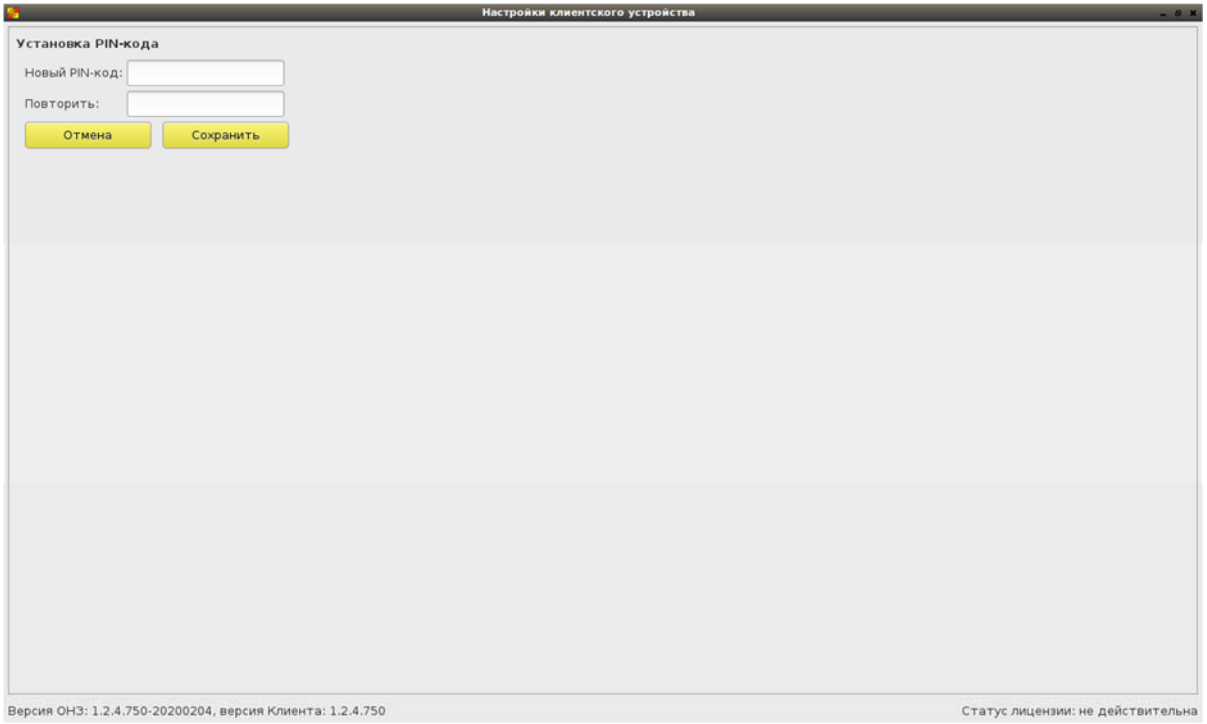

Рисунок 1 – Окно установки PIN-кода Администратора при первом доступе

В окне установки PIN-кода нужно ввести PIN-код с подтверждением и нажать кнопку <Сохранить> (<Enter>). В результате успешной установки появляется оповещение, отраженное на рисунке 2.

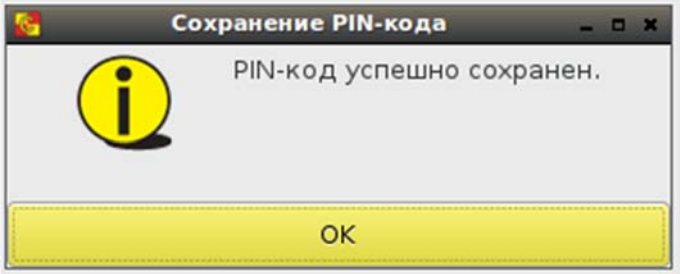

Рисунок 2 – Сообщение об успешной установке PIN-кода

Для продолжения работы следует закрыть информационное окно.

Если PIN-код уже установлен, после загрузки ПО Клиента появляется окно идентификации Администратора (рисунок 3). В этом окне следует ввести корректный PIN-код и нажать кнопку  (<Enter>).

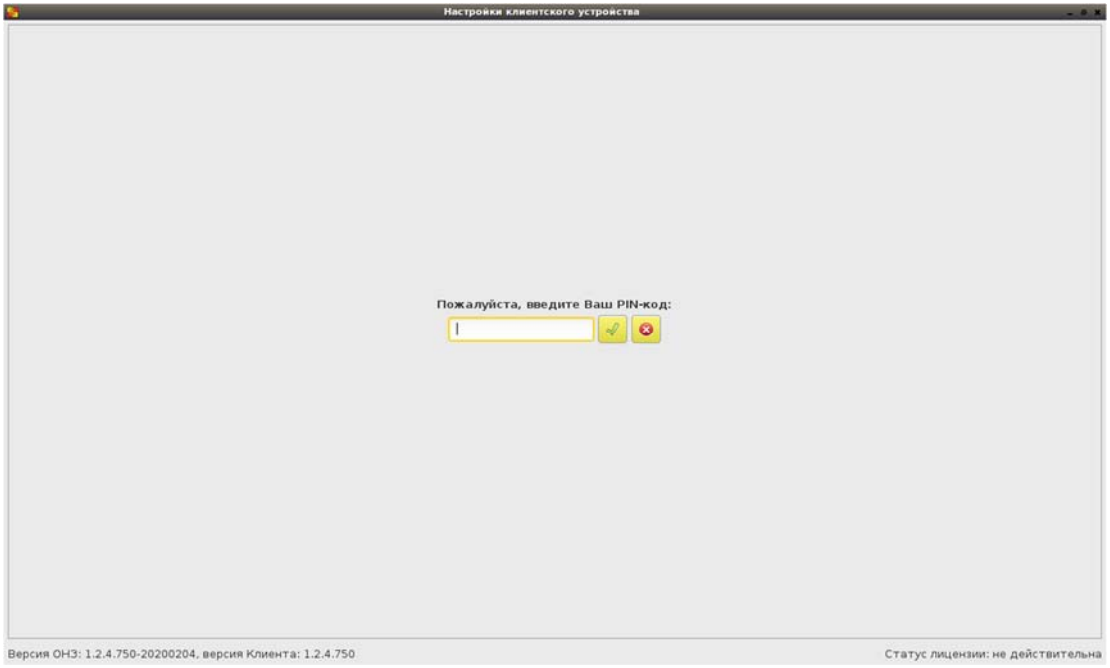

Рисунок 3 – Окно идентификации Администратора

Если введен корректный PIN-код, появляется окно с доступными Администратору клиентского устройства функциями (рисунок 4).

В случае если используемое разрешение монитора не позволяет отобразить все элементы интерфейса Администратора на одном экране, есть возможность использовать прокрутку (с помощью колеса мыши или элемента прокрутки в правой части экрана).

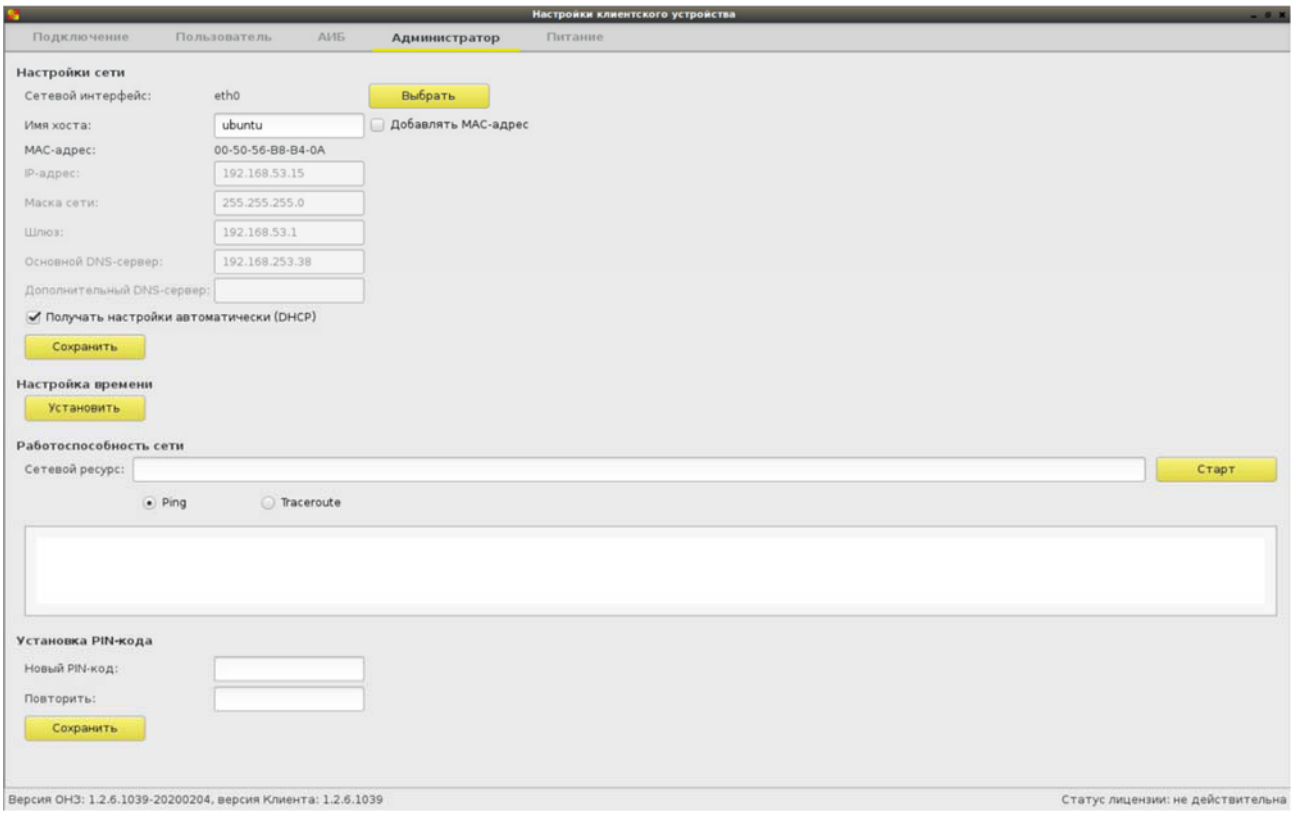

Рисунок 4 – Вкладка «Администратор»

3.4 Установка сетевых настроек Клиента

Установка сетевых настроек Клиента выполняется на вкладке «Администратор» (рисунок 4).

Доступны следующие сетевые настройки:

– «Сетевой интерфейс» - позволяет задать имя используемого сетевого интерфейса.

При первом запуске ПО Клиента указанный параметр не задан. В случае если на СВТ, на котором загружено ПО Клиента, обнаружен единственный интерфейс стандартного типа (eth0, eth1 и т.п.), то этот интерфейс будет задан автоматически. В противном случае (например, СВТ содержит несколько сетевых интерфейсов) при старте ПО Клиента появится окно выбора интерфейса, в котором интерфейс может быть выбран из выпадающего списка (рисунок 5) и задан нажатием кнопки <Выбрать> (рисунок 6). Если окно выбора закрыть, не задав значение интерфейса, то в поле «Сетевой интерфейс» появится значение «не выбран», сетевые настройки не будут применены, а при каждом переключении между вкладками окна «Настройки клиентского устройства» или при обновлении (F5) будет появляться окно напоминания (рисунок 7). Обратите внимание, что для корректной работы Клиента необходимо, чтобы сетевой интерфейс и его параметры были настроены.

Если ранее интерфейс уже был выбран, то при последующих запусках в строке «Сетевой интерфейс» отобразится ранее установленное значение, которое может быть изменено при нажатии на кнопку «Выбрать».

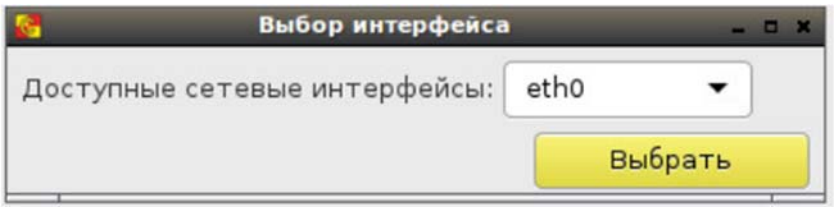

Рисунок 5 - Окно выбора сетевого интерфейса

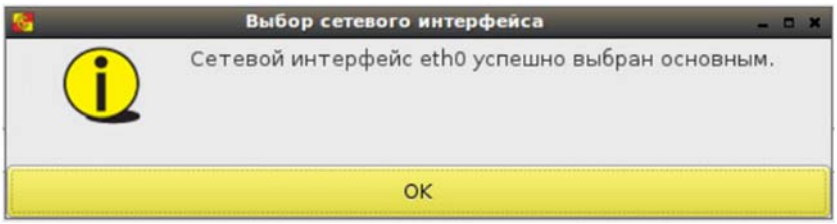

Рисунок 6 - Окно подтверждения выбора сетевого интерфейса

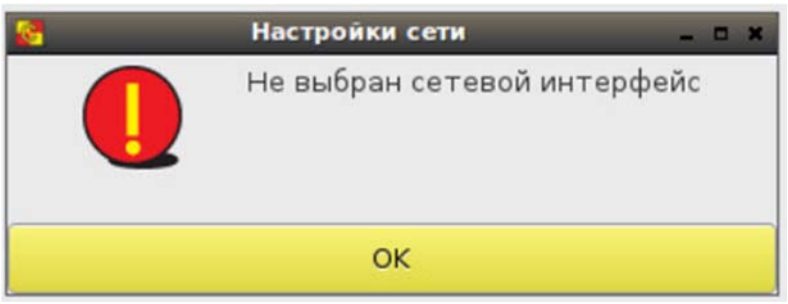

Рисунок 7 - Напоминание о том, что сетевой интерфейс не выбран

– «Получать настройки автоматически (DHCP)» – позволяет включить/выключить функцию получения сетевых настроек Клиента от DHCP-сервера. Если флаг установлен, редактирование значений остальных настроек невозможно, значения устанавливаются автоматически (при условии доступности DHCP-сервера). Если доступный DHCP-сервер отсутствует, необходимо снять данный флаг и указать значения остальных настроек вручную. По умолчанию флаг установлен;

– «Имя хоста» – позволяет задать имя Клиента, которое доступно администратору Citrix;

– «Добавлять MAC-адрес» – позволяет добавить к сетевому имени Клиента его MAC-адрес. При установке флага к имени хоста добавляется MAC-адрес, указанный в строке ниже.

Нижеследующие параметры подлежат настройке при задании сетевого интерфейса:

– «MAC-адрес» – отображает MAC-адрес Клиента;

– «IP-адрес» – позволяет задать IP-адрес Клиента;

– «Маска сети» – позволяет задать маску сети, в которой находится Клиент;

– «Шлюз» – позволяет задать шлюз подсети Клиента;

– «Основной DNS-сервер» – позволяет задать основной DNS-сервер сети Клиента;

– «Дополнительный DNS-сервер» – позволяет задать дополнительный DNS-сервер сети Клиента.

После установки требуемых значений следует нажать кнопку <Сохранить>. В случае успешной установки настроек появляется сообщение, отображенное на рисунке 8.

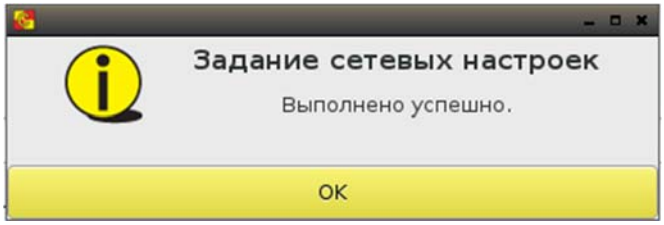

Рисунок 8 – Сообщение об успешной установке сетевых настроек

ВНИМАНИЕ! После установки/снятия флага «Получать настройки автоматически (DHCP)» обязательно сохранять настройки, даже если их значения не изменились.

ПАК «Центр-Т» позволяет проводить диагностику сети. Для использования этой функции в строке «Сетевой ресурс» нужно ввести адрес ресурса, доступность которого необходимо проверить, и выбрать утилиту для проверки – «Ping» или «Traceroute», установив соответствующий флаг. Проверка начинается по кнопке <Старт>.

3.5 Настройки даты и времени

Установка настроек даты и времени Клиента выполняется на вкладке «Администратор» при нажатии кнопки <Установить> раздела «Настройка времени».

В открывшемся окне Администратор может как установить дату и время самостоятельно, так и задать синхронизацию с сервером NTP (рисунок 9).

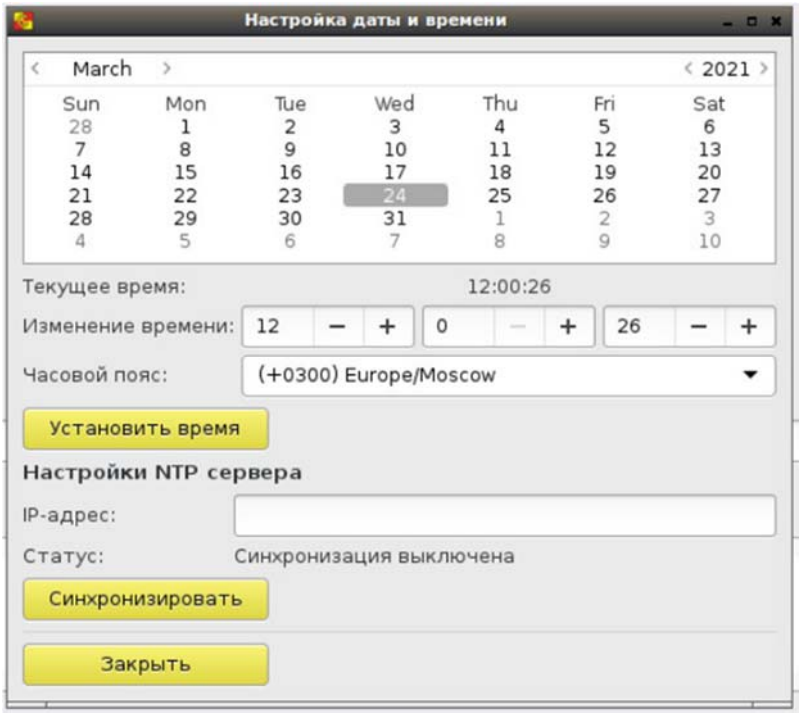

Рисунок 9 - Окно настройки даты и времени Клиента

Администратор может изменить число, месяц и год, а также текущее время и часовой пояс в нижней части окна. Сохранение параметров производится по кнопке <Установить время>.

Установка времени и часового пояса происходит следующим образом:

- при изменении только поля «Изменение времени» меняется и время UTC, и текущее время рабочей станции. Например, был установлен часовой пояс (+0300) и текущее время «12:56:00», то есть время UTC было «09:56:00». В поле «Изменение времени» поменяли значение на «10:56:00», после применения значений текущее время стало «10:56:00», часовой пояс остался по-прежнему (+0300) и время UTC изменилось на «07:56:00»;
- при изменении только поля «Часовой пояс» меняется значение текущего времени, но не время UTC. Например, был установлен часовой пояс (+0300) и текущее время «12:56:00», то есть время UTC было «09:56:00». В поле часовой пояс поменяли значение на (+0100), после применения настроек текущее время изменилось на «10:56:00», часовой пояс стал (+0100), а время UTC не изменилось - осталось «09:56:00»;
- при изменении и поля «Изменение времени», и поля «Часовой пояс» сначала применяются настройки времени, а потом часового

пояса. Например, был установлен часовой пояс (+0300) и текущее время «12:56:00», то есть время UTC было «09:56:00». Задали в поле «Изменение времени» «10:00:00», а в поле «Часовой пояс» - (+0400). После применения настроек произошло следующее: сначала в соответствии с заданным в поле «Изменение времени» параметром поменялось текущее время и время в UTC (текущее стало «10:00:00», UTC – «07:00:00»), после применилось значение часового пояса, и в итоге текущее время стало «11:00:00», UTC «07:00:00» и часовой пояс (+0400).

Также для настройки даты и времени может использоваться внешний NTP сервер. Для его использования необходимо заполнить поле «IP-адрес» раздела «Настройки NTP сервера» и нажать кнопку <Синхронизировать>. Поле «Статус» отображает текущее состояние синхронизации.

При вводе IP-адреса проводится проверка на корректность его формата, и в случае указания неверного формата выдается соответствующее сообщение (рисунок 10).

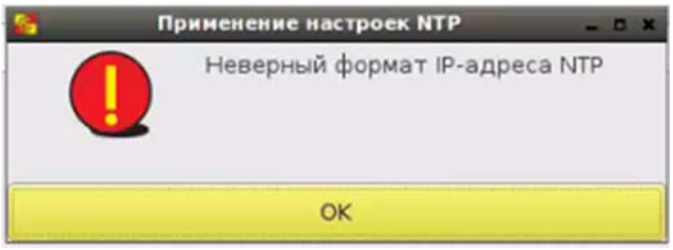

Рисунок 10 - Сообщение при вводе неверного формата IP-адреса

После задания и сохранения параметров необходимо нажать кнопку <Закрыть> для завершения работы с настройками даты и времени.

3.6 Смена PIN-кода Администратора

Смена PIN-кода Администратора выполняется на вкладке «Администратор» в нижней части окна (рисунок 4). Здесь необходимо ввести новый PIN-код с подтверждением и нажать кнопку <Сохранить> (<Enter>).

В результате успешного выполнения процедуры появляется окно с сообщением о сохранении PIN-кода (рисунок 2).

4 Состав работ Администратора безопасности информации клиентских устройств

4.1 Общие сведения

После получения клиентского устройства Администратор БИ должен:

1) получить доступ к ПО Клиента и установить PIN-код Администратора БИ при первом доступе (см. 4.2);

2) установить сетевые настройки СХСЗ (см. 4.3).

В процессе эксплуатации Комплекса Администратор БИ может управлять отладочным режимом (см. 4.3), при необходимости копировать файл лицензии со съемного носителя на клиентское устройство (см. 4.4), производить резервирование и восстановление локальных настроек Клиента (см. 4.5 и 4.6), просматривать локальные события безопасности (см. 4.7) и изменять свой PIN-код (см. 4.8).

4.2 Получение доступа к ПО Клиента

Процедура получения доступа Администратора БИ к ПО Клиента выполняется в целом так же, как и аналогичная процедура для Администратора (см. 3.3). Отличие состоит в том, что для доступа к функциям администрирования Администратор БИ клиентского устройства должен перейти на вкладку «АИБ» и выполнить здесь установку собственного PIN-кода при первом доступе к ПО Клиента.

Если PIN-код уже установлен, после загрузки ПО Клиента появляется окно идентификации Администратора БИ (рисунок 3).

В случае ввода корректного PIN-кода в окне идентификации Администратора БИ на экране появляется окно с доступными Администратору БИ функциями (рисунок 11).

В случае если используемое разрешение монитора не позволяет отобразить все элементы интерфейса Администратора БИ на одном экране, есть возможность использовать прокрутку (с помощью колеса мыши или элемента прокрутки в правой части экрана).

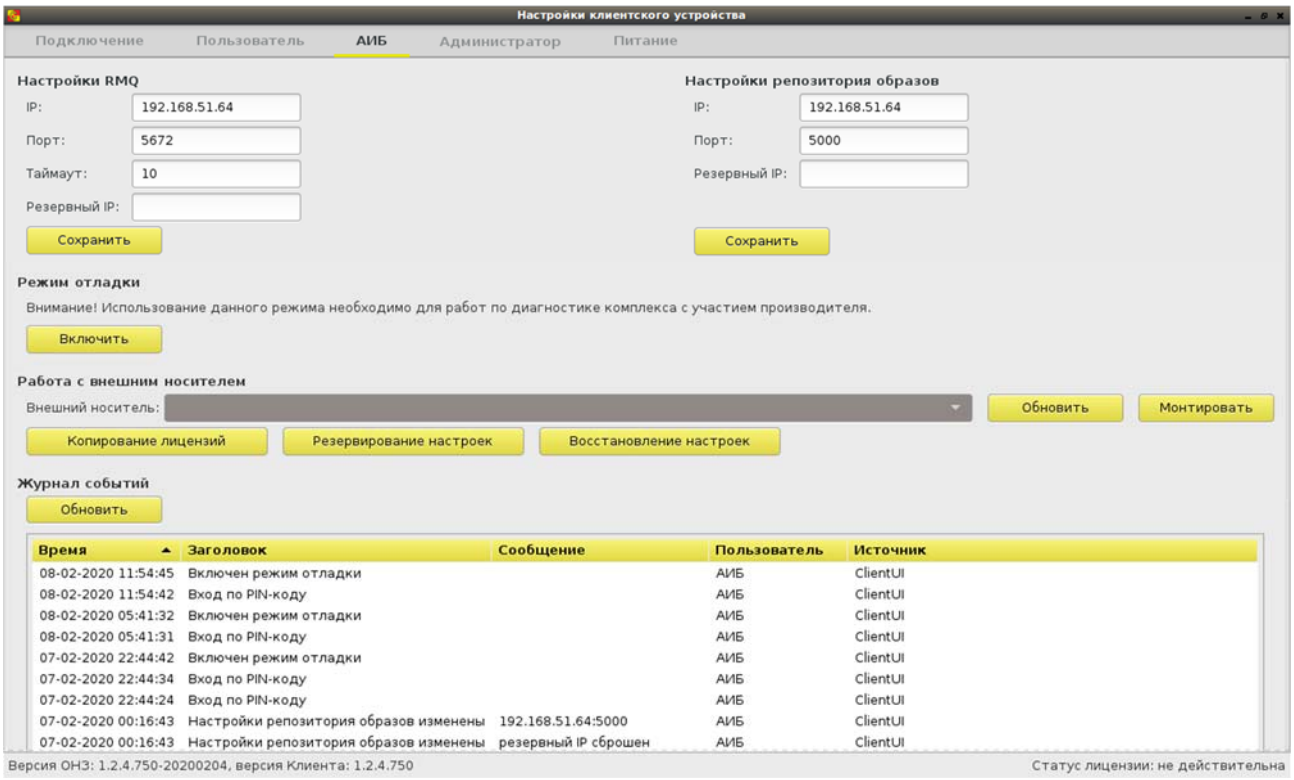

Рисунок 11 – Вкладка «АИБ» с доступными Администратору БИ функциями

4.3 Установка сетевых настроек СХСЗ

Установка сетевых настроек СХСЗ выполняется на вкладке «АИБ» (рисунок 11).

Доступны следующие сетевые настройки:

- *«Настройки RMQ»:*
  - «IP» – позволяет указать адрес в сети брокера сообщений, используемого СХСЗ;
  - «Порт» – позволяет указать порт брокера сообщений, используемого СХСЗ;
  - «Тайм-аут» – позволяет указать время ожидания отклика от брокера сообщений в секундах;
  - Резервный IP – позволяет указать адрес в сети брокера сообщений, используемого резервным СХСЗ (необязательный параметр).
- *«Настройки репозитория образов»*:
  - «IP» – позволяет указать адрес в сети БД с образами ПО ТС, развернутой на СХСЗ;
  - «Порт» – позволяет указать порт БД с образами ПО ТС, развернутой на СХСЗ;
  - Резервный IP – позволяет указать порт БД с образами ПО ТС, развернутой на резервном СХСЗ (необязательный параметр).

ВНИМАНИЕ! Номера портов БД с образами ПО ТС, развернутых на основном и резервном СХСЗ, должны совпадать.

Значения адреса и порта RMQ и БД с образами ПО ТС необходимо узнать у Администратора сервисного режима СХСЗ. Если брокер сообщений и репозиторий образов находятся на одном СХСЗ, необходимо указывать один и тот же IP-адрес. По умолчанию для RMQ установлен порт 5672, а для репозитория образов – 5000.

После установки требуемых значений следует нажать кнопку <Сохранить>.

При успешном сохранении настроек RMQ и репозитория образов появляются соответствующие сообщения (рисунки 12 и 13).

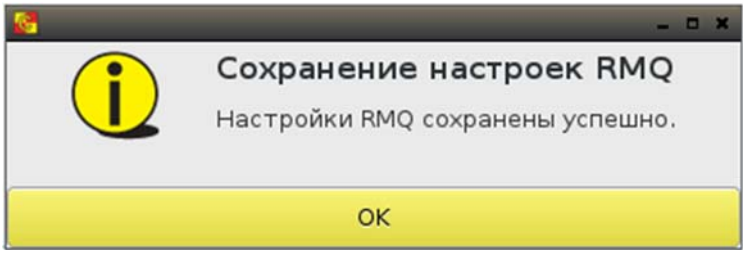

Рисунок 12 – Сообщение об успешном сохранении настроек RMQ

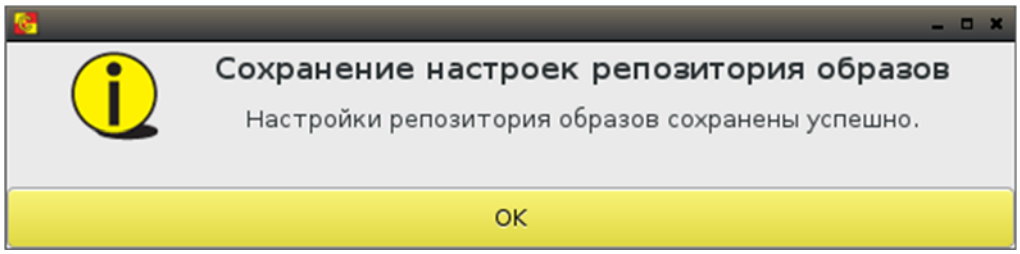

Рисунок 13 – Сообщение об успешном сохранении настроек репозитория образов

Также есть возможность перехода в режим отладки, необходимый для работ по диагностике Комплекса с участием производителя. По умолчанию данный режим отключен.

Примечание: *Если в системе предусмотрено АРМ Эмиссии, часть сетевых настроек СХСЗ может выполнять администратор АРМ Эмиссии (подробнее см. Руководство по эксплуатации АРМ Эмиссии 37222406.26.20.40.140.042 92).*

4.4 Копирование лицензии

Носители с записанным на них образом Клиента поставляются с уже записанной лицензией, и данный этап настройки может быть пропущен.

В случае, если запись ОНЗ на носитель Клиента производилась Администратором, Администратор БИ клиентского устройства должен перенести файл лицензии со съемного носителя на клиентское устройство.

ВНИМАНИЕ! Внешний носитель должен иметь файловую систему NTFS и имя «centertusb» (обязательно строчными буквами) или файловую систему FAT и имя «centertusb» (регистр не имеет значения).

На внешнем носителе должен быть создан каталог «lic», в который необходимо скопировать лицензию. Монтирование внешнего носителя происходит в поле «Работа с внешним носителем» вкладки АИБ (рисунок 11).

После подключения внешнего носителя следует нажать кнопку <Обновить> (F5), далее выбрать его имя в выпадающем списке строки «Внешний носитель» и нажать кнопку <Монтировать> (рисунок 14).

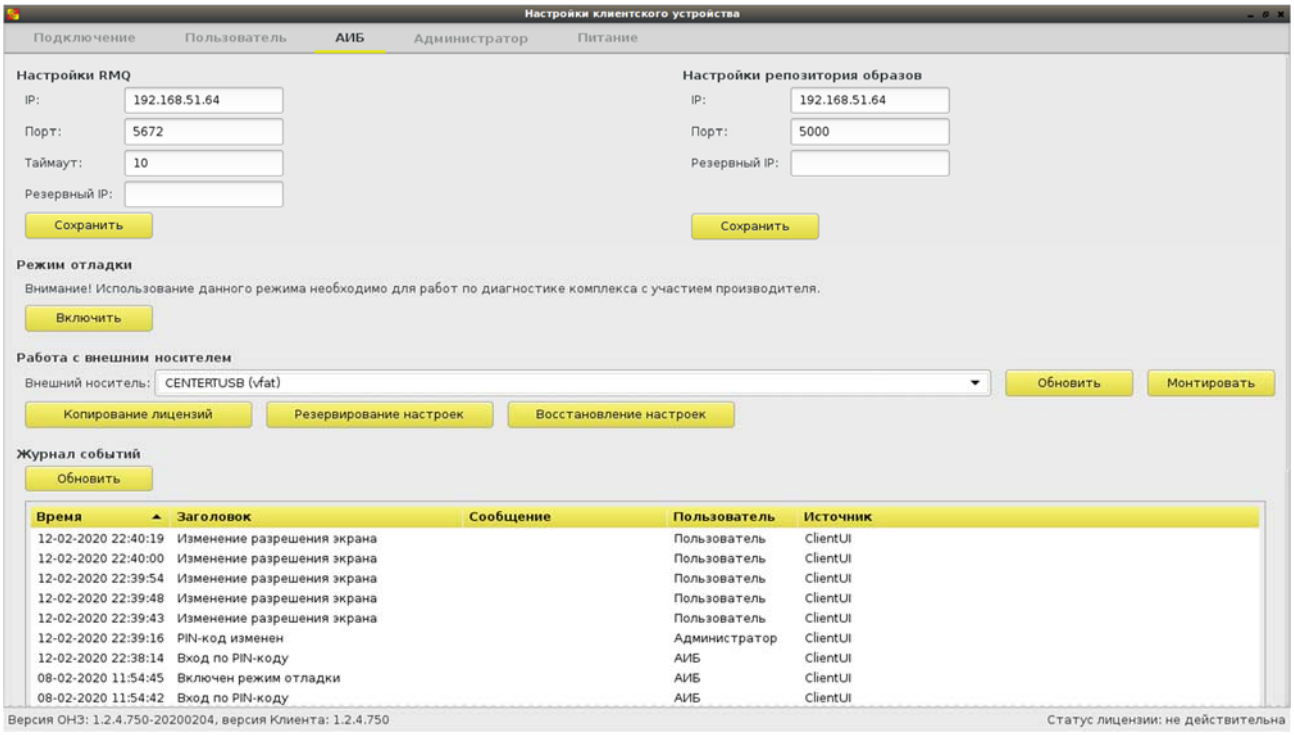

Рисунок 14 – Монтирование внешнего носителя

Далее нажать кнопку <Копирование лицензий>.

Если внешний носитель не был примонтирован (или не был подключен), появится окно, предупреждающее о необходимости его монтирования (рисунок 15).

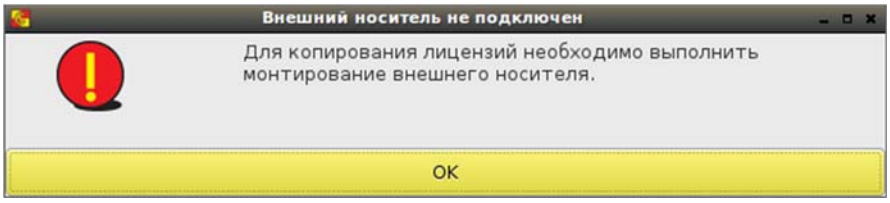

Рисунок 15 – Окно, предупреждающее о необходимости монтирования внешнего носителя

В случае успешного монтирования появляется окно «Копирование лицензий», в котором будут отображены все файлы лицензий из каталога «lic» внешнего носителя.

При выборе лицензии из списка становится активной кнопка «Скопировать» (рисунок 16), при нажатии на которую произойдет перенос файла на клиентское устройство и появится информационное сообщение о

копировании (рисунок 17). Такое же сообщение о копировании лицензии появится в журнале событий Администратора БИ.

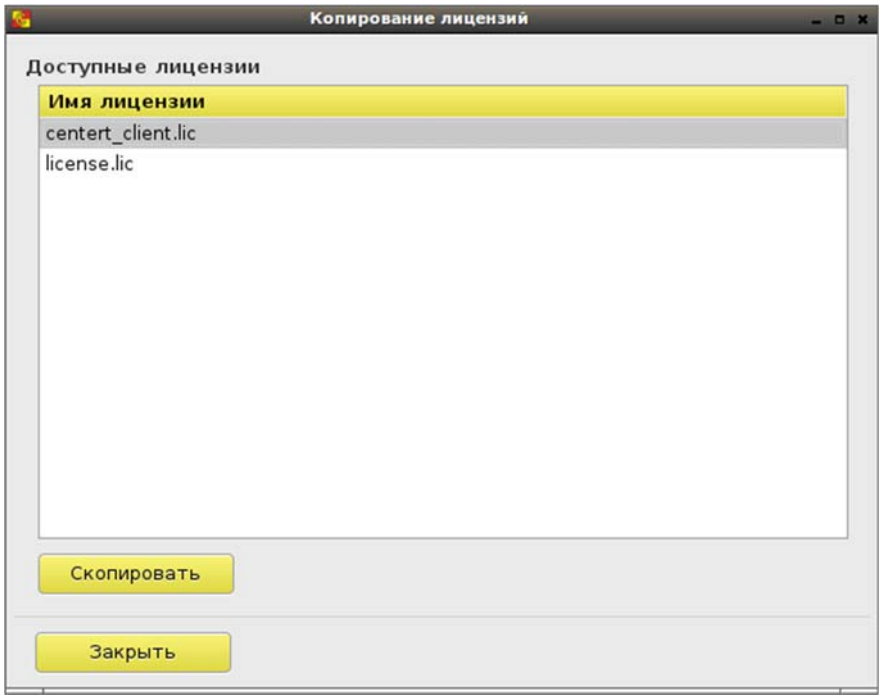

Рисунок 16 - Выбор файла лицензии для копирования на клиентское устройство

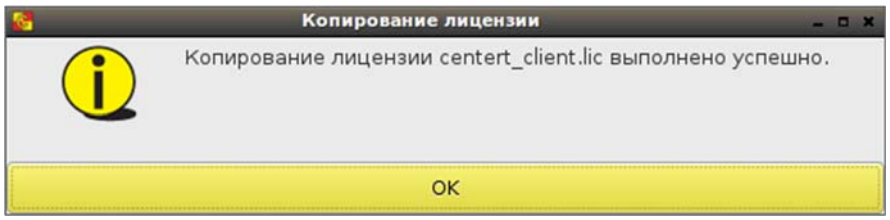

Рисунок 17 - Сообщение об успешном копировании лицензии

Если на устройстве уже есть файл лицензии, будет выведено сообщение с предложением заменить его на выбранный файл (рисунок 18).

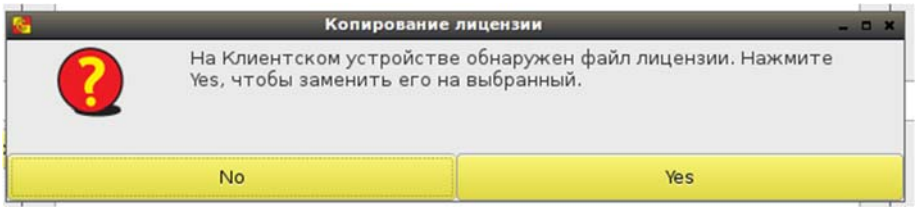

Рисунок 18 – Сообщение о наличии на устройстве файла лицензии

Перезагрузка Клиента не требуется.

Статус лицензии отображается в нижней строке экрана, в правой части – «действительна» или «недействительна». Если скопированная лицензия недействительна, соответствующее сообщение с указанием причины, по которой указанная лицензия не подходит для клиентского устройства, будет выведено при переходе между вкладками (рисунок 19).

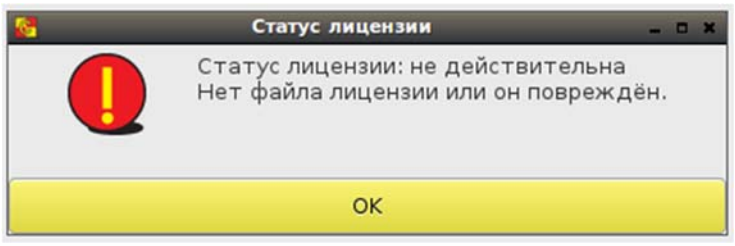

Рисунок 19 - Сообщение о статусе лицензии «недействительна»

Статус лицензии «недействительна» не ограничивает работоспособность клиентского устройства.

Если файл лицензии не был скопирован, или он поврежден, или недействителен по какой-либо другой причине, это будет также отображено в журнале «Сервис управления» и в Утилите удаленного администрирования СХСЗ.

4.5 Резервирование локальных настроек Клиента

Администратор БИ может выполнять резервирование локальных настроек клиентского устройства и последующее восстановление их.

Для получения возможности резервирования настроек необходимо подключить и примонтировать к клиентскому устройству внешний носитель, на котором должен находиться каталог «backups_client» (подробнее о монтировании внешнего носителя - п. 4.4). Далее при нажатии кнопки <Резервирование настроек> (рисунок 14) появляется окно выбора параметров для резервирования (рисунок 20).

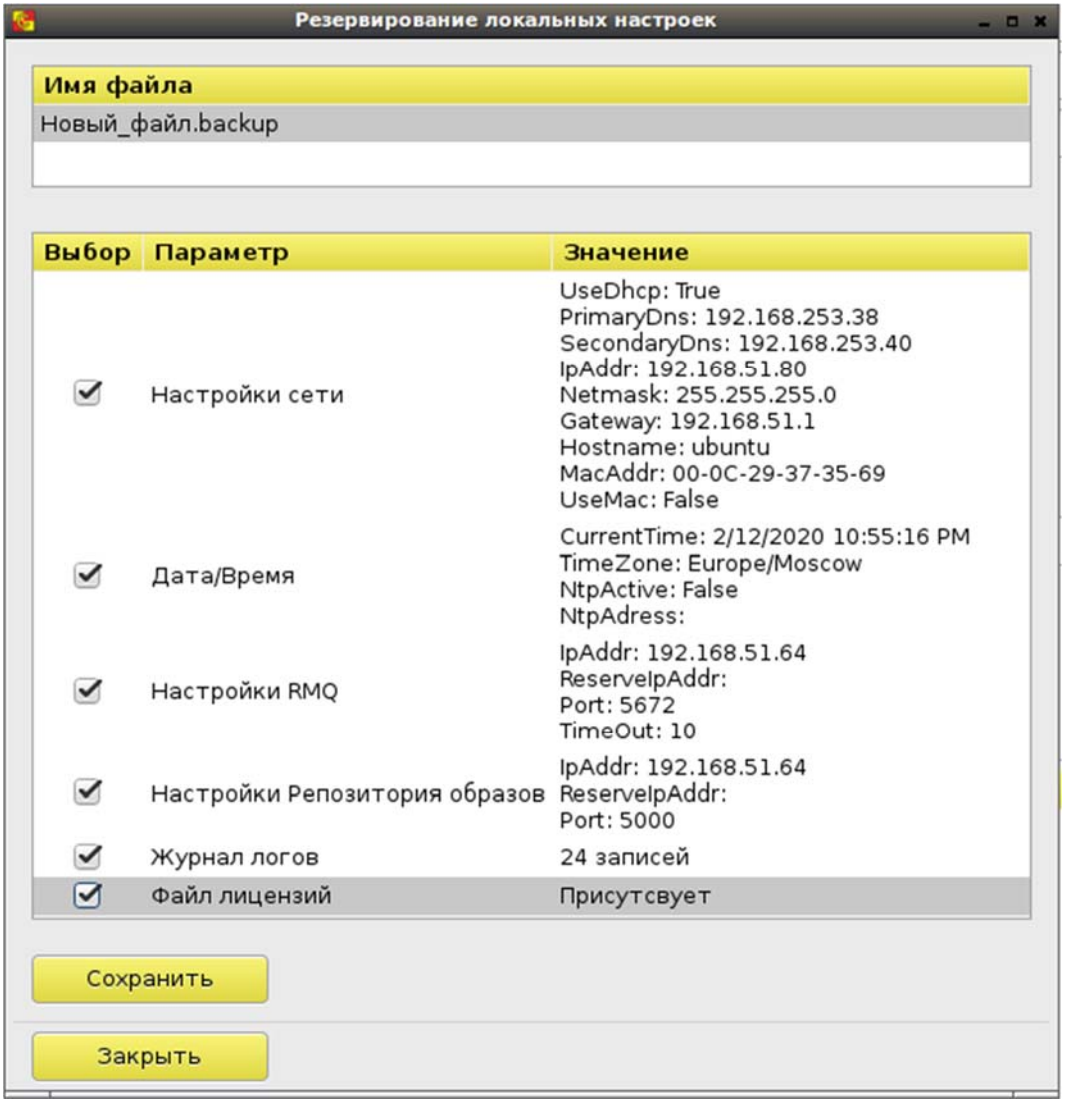

Рисунок 20 – Окно выбора настроек для резервирования

В этом окне есть возможность выбора нужных параметров резервирования. Все значения параметров будут заноситься в резерв в том виде, в каком описаны в окне, за исключением журнала логов, в строке которого указано только число записей, заносимых в резерв. Нет необходимости в резервировании лицензии при ее отсутствии.

После выбора параметров следует нажать кнопку <Сохранить>.

Об успешном завершении процедуры резервирования свидетельствует соответствующее сообщение (рисунок 21), в котором отражены все выбранные параметры. Имя файла резервной копии формируется из серийного номера клиентского устройства и меток даты и времени. Окно резервирования локальных настроек закрывается кнопкой <Закрыть>, при этом в журнале событий регистрируется сообщение об изменении настроек репозитория образов (рисунок 22).

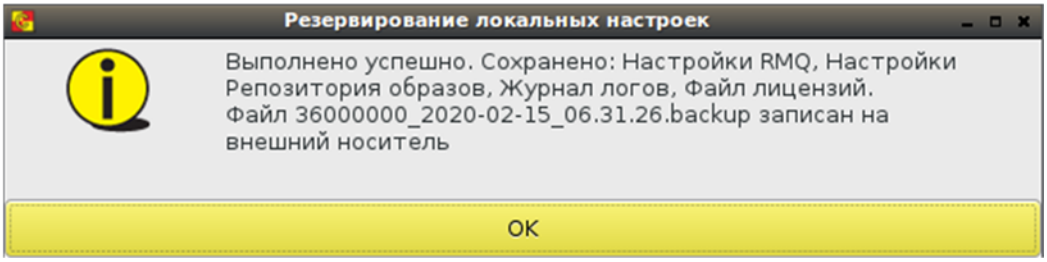

Рисунок 21 – Сообщение об успешном выполнении резервирования настроек

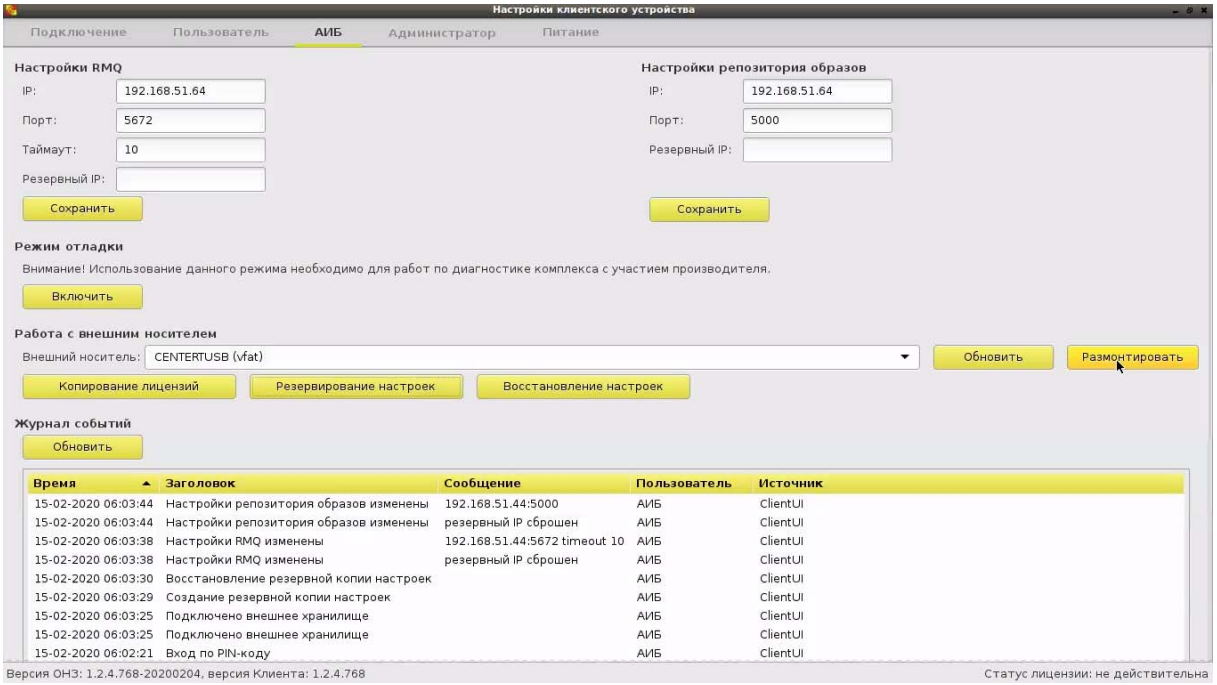

Рисунок 22 – Завершение процедуры резервирования

Далее внешний носитель следует размонтировать, последовательно нажав кнопки <Размонтировать> и <Обновить> (F5) (рисунок 22), при этом его необязательно отключать от клиентского устройства.

4.6 Восстановление резервной копии настроек Клиента

При необходимости восстановления настроек Клиента из резервной копии внешний носитель с каталогом «backups_client» следует примонтировать к клиентскому устройству (подробнее о монтировании внешнего носителя - п. 4.4) и нажать кнопку <Восстановление настроек> (рисунок 14). Появляется окно восстановления локальных настроек (рисунок 23).

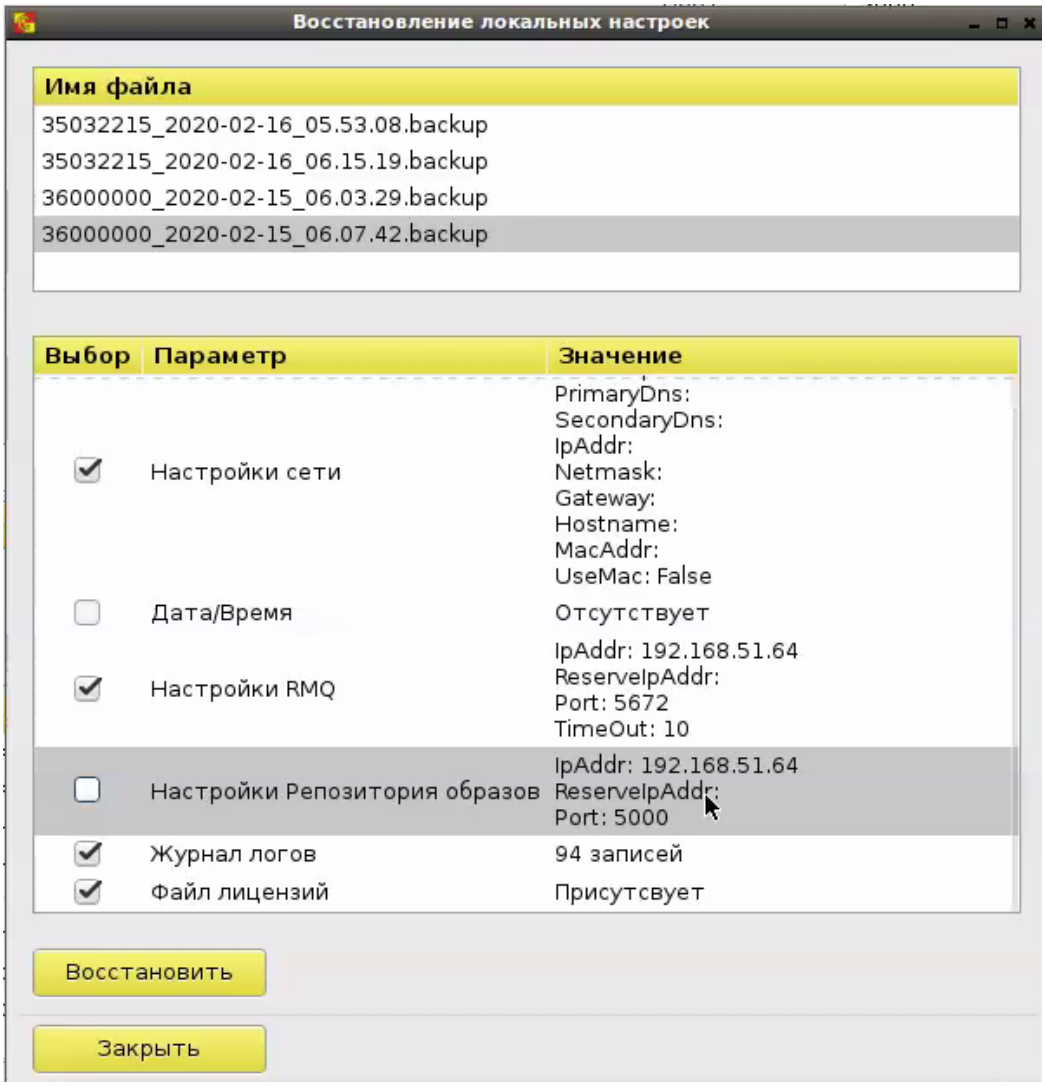

Рисунок 23 – Окно восстановления локальных настроек

В поле «Имя файла» показан список ранее сохраненных резервных копий настроек. Выбрать нужный файл можно по его имени, в котором записаны серийный номер клиентского устройства и метки даты и времени. При выборе файла в нижнем поле отображаются значения сохраненных в нем параметров. Допускается восстановление части параметров. В этом случае следует оставить метку выбора только в строке параметров, требующих восстановления.

После выбора файла и параметров восстановления необходимо нажать кнопку <Восстановить>. В сообщении об успешном восстановлении настроек отражены все восстановленные параметры (рисунок 24).

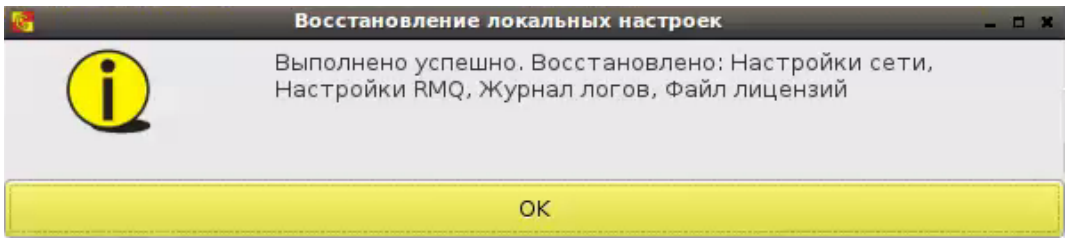

Рисунок 24 – Сообщение об успешном восстановлении настроек

Обратите внимание, что при восстановлении журнала логов из резервной копии в нем могут появиться дублирующие записи, так как события журнала при его резервировании не удаляются.

Окно восстановления локальных настроек закрывается кнопкой <Закрыть>, при этом в журнале событий регистрируется сообщение о восстановлении резервной копии настроек.

4.7 Просмотр событий безопасности

Администратор БИ клиентского устройства может просматривать записи журнала о локальных событиях безопасности, отображающие действия администраторов и Пользователя клиентского устройства.

Просмотреть записи журнала можно в нижней части окна вкладки «АИБ» (рисунок 11).

Для каждого события фиксируются:

- время;
- заголовок (основная информация о событии);
- сообщение;
- пользователь (учетная запись, от имени которой выполнено действие);
- источник события.

После каждого обращения к СХСЗ новые записи из журналов клиентских устройств копируются в журнал СХСЗ, доступный Администратору БИ СХСЗ. Если Администратор СХСЗ установил для данного клиентского устройства флаг «Удалять события после передачи их на сервер», после каждого обращения к серверу с запросом на получение образа ПО ТС журнал событий клиентского устройства очищается.

ВНИМАНИЕ! Для корректного отображения времени в записях о событиях безопасности, получаемых СХСЗ от клиентских СВТ, на клиентских СВТ в BIOS должно быть установлено время по UTC-зоне.

4.8 Смена PIN-кода Администратора БИ

Смена PIN-кода Администратора БИ выполняется на вкладке «АИБ» в нижней части окна. Необходимо ввести новый PIN-код с подтверждением и нажать кнопку <Сохранить>.

В результате успешного выполнения процедуры появляется окно с сообщением о сохранении PIN-кода (рисунок 2).

5 Состав работ пользователей клиентских устройств

5.1 Общие сведения

При получении клиентского устройства Пользователь:

1) осуществляет загрузку СВТ в режиме работы с ПАК «Центр-Т» и получает доступ к ПО Клиента (см. 5.2);

2) работает в рамках терминальной сессии (см. 5.3).

В процессе эксплуатации Комплекса Пользователь может изменить разрешение экрана, просмотреть сетевые настройки Клиента (см. 5.5) и проверить работоспособность сетевого ресурса (см.5.6).

5.2 Получение доступа к ПО Клиента

Процедура получения Пользователем доступа к ПО Клиента выполняется в целом так же, как и аналогичная процедура для Администратора (см. 3.3). Отличие состоит в том, что основная работа Пользователя выполняется на вкладках «Подключение» и «Пользователь».

ВНИМАНИЕ! В случае использования ключевого носителя vdToken его следует подключать после загрузки ПО Клиента.

Для выполнения собственных функций Пользователю не требуется PIN-код, как для администраторов клиентских устройств.

Если Администраторами удаленного управления СХСЗ установлены настройки подключения, Пользователю можно перейти к загрузке образа ПО ТС (см. 5.3).

5.3 Работа в рамках терминальной сессии

Каждому Пользователю Администраторами удаленного управления СХСЗ могут быть назначены одна или несколько пар «Образ/шаблон». Каждая такая пара определяет терминальную сессию (подключение), которая может быть открыта Пользователем. Терминальная сессия характеризуется двумя параметрами: с каким терминальным сервером Citrix (задается в шаблоне настроек ПО ТС) может работать Пользователь и как будет осуществляться подключение к этому терминальному серверу (определяется назначенным образом ПО ТС). Также для Пользователя определяется максимальное число одновременных подключений к терминальным серверам (терминальных сессий), которые могут быть открыты на клиентском устройстве.

При старте ПО Клиента автоматически начинается подготовка Клиента к старту терминальной сессии (подключение к СХСЗ, получение от него назначенных Пользователю образов и шаблонов настроек ПО ТС и т.д.). На этом этапе возможны следующие ошибки при установке синхронизации с СХСЗ:

- если СХСЗ виртуальный, и к нему не подключен Специальный носитель ПО ПАК «Центр-Т»[3];

- если Пользователь заблокирован.

При успешном старте ПО по умолчанию с СХСЗ начинается скачивание всех образов ПО ТС, назначенных Пользователю и имеющих подходящую для работы архитектуру, и открытие всех доступных для него терминальных сессий (подключений). Отладочная информация о подготовке Клиента к началу терминальной сессии (ход подключения к СХСЗ, загрузка образов и шаблонов настроек ПО ТС с СХСЗ, старт терминальных сессий) по умолчанию скрыта, в строке «Статус» отображается лишь краткая информация о ходе подключения (рисунок 25). Для отображения всей информации необходимо раскрыть список «Подробнее» (рисунок 26, рисунок 27).

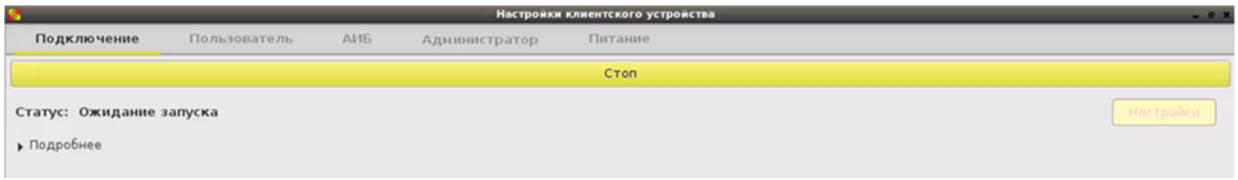

Рисунок 25 - Подготовка к старту терминальной сессии. Отладочная информация скрыта

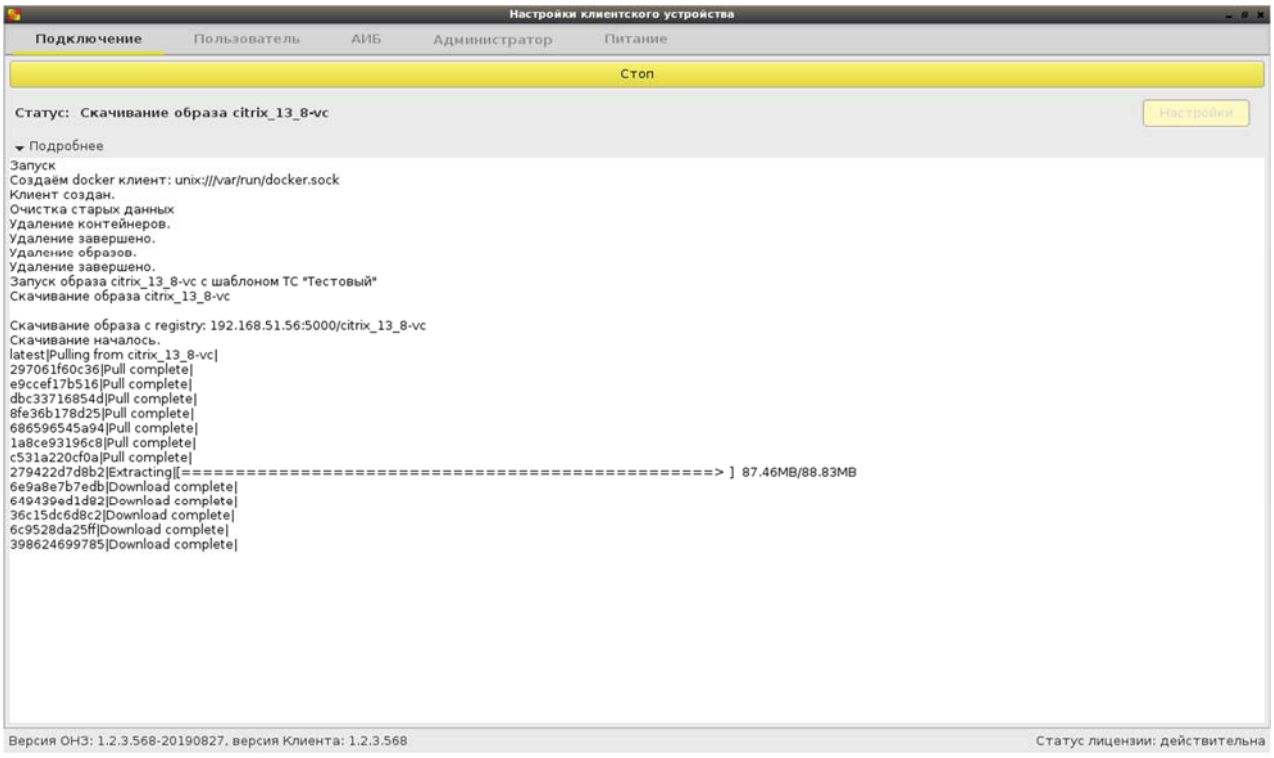

Рисунок 26 - Подготовка к старту терминальной сессии. Список «Подробнее»

[3] Возможность использования виртуального СХСЗ появилась в версии 1.2.10. Его работа обеспечивается только при постоянно подключенном Специальном носителе ПО ПАК «Центр-Т»

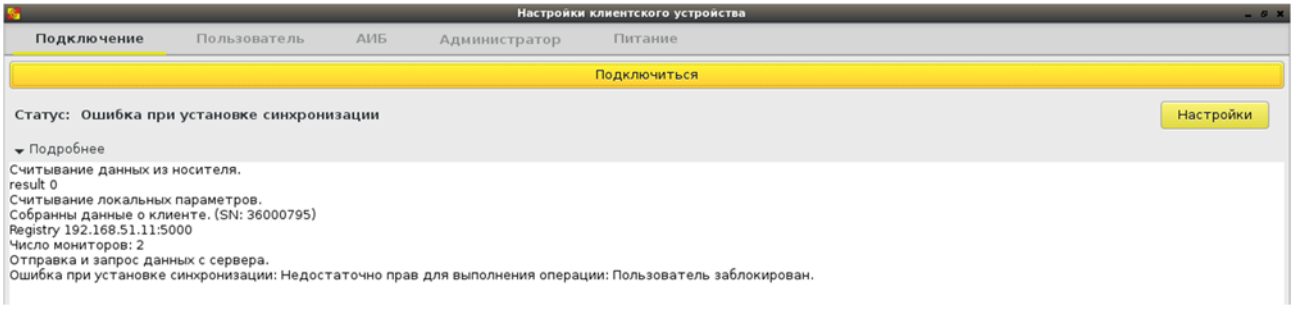

Рисунок 27 – Список «Подробнее» при попытке подключиться заблокированному пользователю

Если Пользователь хочет выбрать лишь некоторые из доступных ему подключений, следует остановить начатое подключение к СХСЗ (кнопка «Стоп»), после чего нажать «Настройки». В открывшемся окне (рисунок 28) будут отображены доступные Пользователю подключения (назначенные ему пары «Образ/Шаблон»), указана архитектура используемой терминальной станции («Текущая архитектура»), а также заданное для него максимальное число одновременных подключений. При выборе необходимых подключений следует проверять соответствие текущей архитектуры архитектуре выбираемого образа, а также учитывать, что при работе на Центр-TrusT число одновременных подключений не должно превышать двух. После сделанного выбора Пользователю следует нажать кнопку «Применить» и возобновить подключение к СХСЗ кнопкой «Подключиться» (рисунок 29). Информация о выбранных подключениях будет передана на СХСЗ, и при следующем старте подключения Пользователя начнется скачивание и запуск тех образов ПО ТС, что были выбраны ранее и имеют подходящую архитектуру.

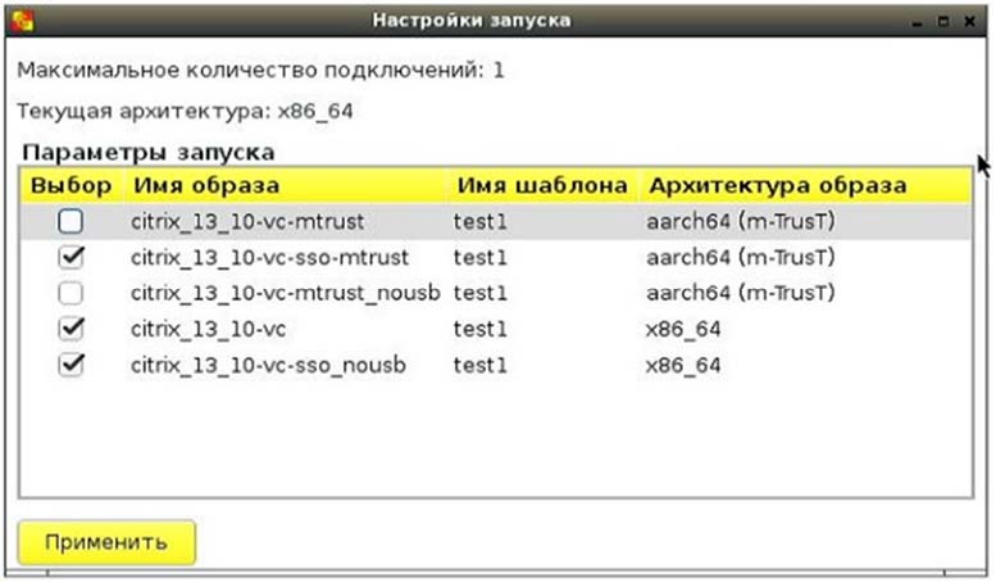

Рисунок 28 - Редактирование параметров запуска в окне «Настройки запуска»

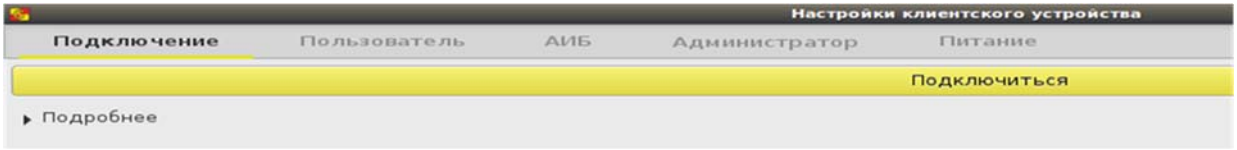

Рисунок 29 - Кнопка <Подключиться>

Если при установке подключения с СХЗС среди назначенных и выбранных для запуска образов нет ни одного образа с подходящей для работы архитектурой, то окно со всеми назначенными для Пользователя образами откроется автоматически (рисунок 30), и после закрытия этого окна в строке «Статус» появится сообщение «Не выбран ни один образ, подходящий для данной архитектуры. Отмена запуска» (рисунок 31).

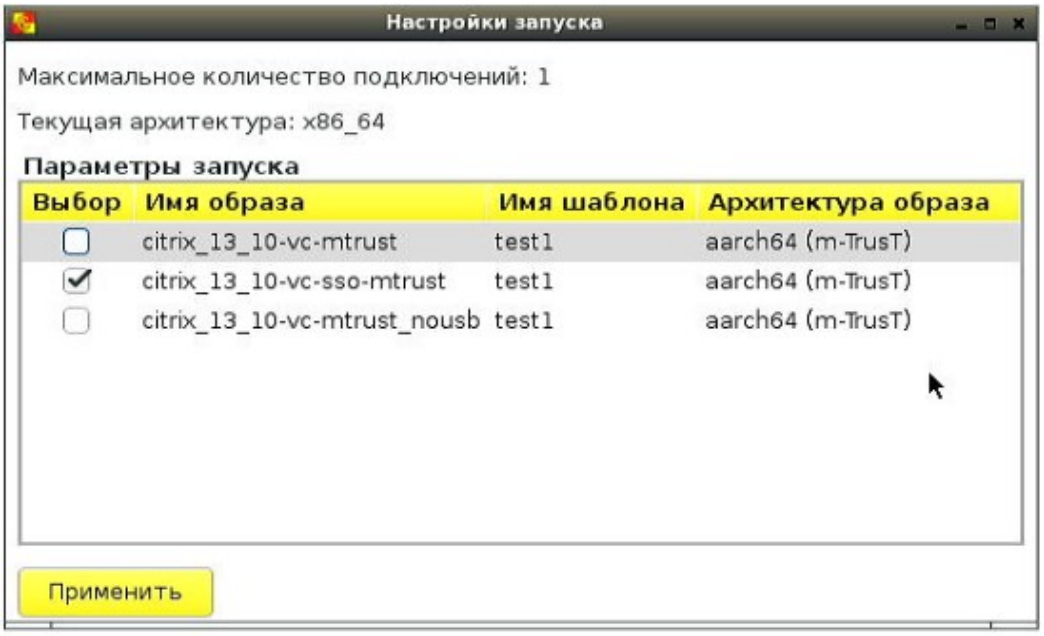

Рисунок 30 - Окно настроек запуска при несовпадении архитектур образа и терминала

Рисунок 31 – Сообщение об отмене запуска при отсутствии подходящего по архитектуре образа

Для изменения выбранных подключений необходимо повторно открыть окно «Настройки запуска» и внести изменения.

Если Администратор БИ СХСЗ установил для Пользователя кэширование образа, образ ПО ТС загружается с СХСЗ только при первой загрузке, в дальнейшем загрузка осуществляется с носителя ПО Клиента. После этого такой способ загрузки используется до тех пор, пока образ ПО ТС, соответствующий Пользователю, не будет изменен.

Если процесс загрузки и проверки образа ПО ТС завершается успешно, начинается загрузка клиентского приложения, инициирующего соединение с терминальным сервером.

Далее начинается работа в рамках терминальной сессии (терминальных сессий).

При старте работы клиентского устройства пользователю может быть отправлено текстовое сообщение от Администратора ИБ. Оно появляется поверх всех открытых подключений или однократно, или при каждом старте. Подобные оповещения могут также приходить в любой момент времени.

Если открыто несколько терминальных сессий, для переключения между окнами сессий следует использовать сочетание клавиш <Ctrl> и <Tab>. При этом для каждого подключения отобразится имя шаблона настроек ПО ТС, используемое при его создании (рисунок 32), а при его выборе (в зависимости от подключаемого образа) будут запрашиваться логин/пароль/считыватель ключа/PIN-код ключа и т.д.

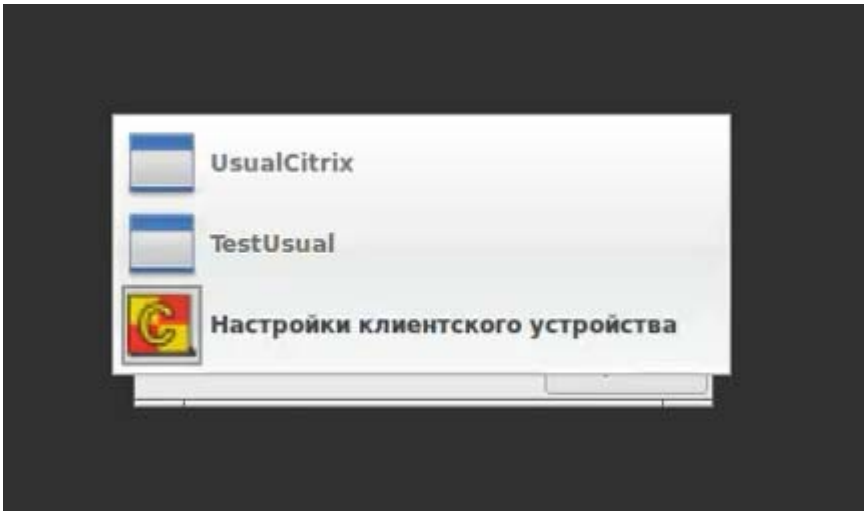

Рисунок 32 - Выбор подключения к терминальному серверу при использовании Защищенного терминала Центр-TrusT

Для возврата к ПО Клиента следует в окне сессии нажатием клавиши <F8> вызвать контекстное меню, в котором выбрать команду «Exit viewer» (рисунок 33).

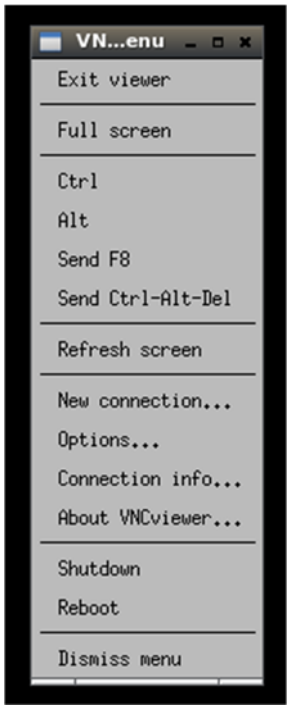

Рисунок 33 – Меню окна терминальной сессии

Если в рамках терминальной сессии планируется использование CCID-устройств, в частности, ключевых носителей типа vdToken, их необходимо

подключить к ТС до начала ICA сессии. Если подключение CCID-устройства произошло после, оно становится недоступным.

Чтобы CCID-устройства вновь стали доступными в рамках терминальной сессии, необходимо перезапустить сессию[4].

ВНИМАНИЕ! Если пароль Пользователя содержит русские буквы, то для переключения раскладки клавиатуры до входа на терминальный сервер следует использовать сочетание клавиш «LEFT SHIFT + RIGHT SHIFT». После авторизации Пользователя на терминальном сервере переключение раскладки клавиатуры происходит в соответствии с настройками сервера (обычно используются сочетания клавиш «ALT+SHIFT» или «CTRL+SHIFT»).

Возможность проброса внешних флеш-накопителей (USB-устройств) в терминальную сессию определяется образом, назначенным Пользователю клиентского устройства. В случае если имя образа имеет постфикс «nousb», проброс запрещен, в противном случае – разрешен проброс любых флеш-накопителей (USB-устройств).

ВНИМАНИЕ! Для проброса накопителей они должны быть подключены после входа Пользователя на терминальный сервер. Если накопитель уже был подключен, необходимо отключить его от терминала и подключить заново.

5.4 Изменение разрешения и тайм-аута гашения экрана

Изменение разрешения экрана производится на вкладке «Пользователь» (рисунок 35) в разделе «Персонализация».

Возможна работа с одним или двумя мониторами.

ВНИМАНИЕ! При работе с терминалом HP510t возможна работа только с одним монитором. Подробнее см. Приложение 1.

Для каждого монитора доступна настройка его включения или отключения (флаг «Включен»), а также изменение разрешения экрана.

Для настройки разрешения экрана монитора следует в строке «Разрешение:» выбрать нужное значение параметра из выпадающего списка. При работе с двумя мониторами, имеющими разные разрешения экрана, возможно изменение размера изображения на втором мониторе при подключении к терминальному серверу. В этом случае разрешение экрана следует скорректировать.

Обратите внимание, что из-за особенностей взаимодействия мониторов и терминальных станций монитор, отключенный от сети электропитания, но подключенный к терминальной станции, отображается как включенный и доступный для настройки. Для устранения некорректного

[4] Это обусловлено особенностями работы Citrix и CCID-устройств (для получения более подробной информации о работе редактора подключений Citrix и CCID-устройств см. http://support.citrix.com/article/CTX132230).

изображения при отключении монитора от электропитания следует отсоединить его и от терминальной станции.

Также обратите внимание, что отключить (снять флаг «Включен») все мониторы невозможно - такое действие будет заблокировано (рисунок 34), так как может привести к недоступности Клиента.

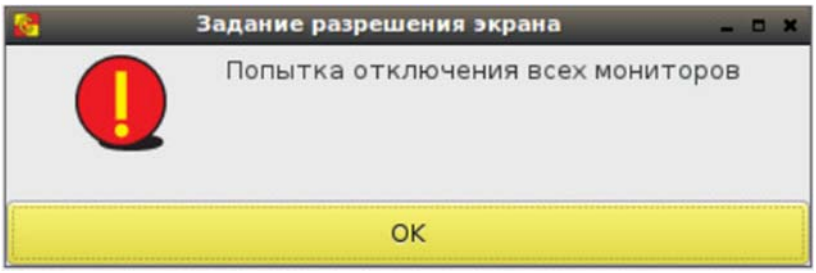

Рисунок 34 – Сообщение об ошибке

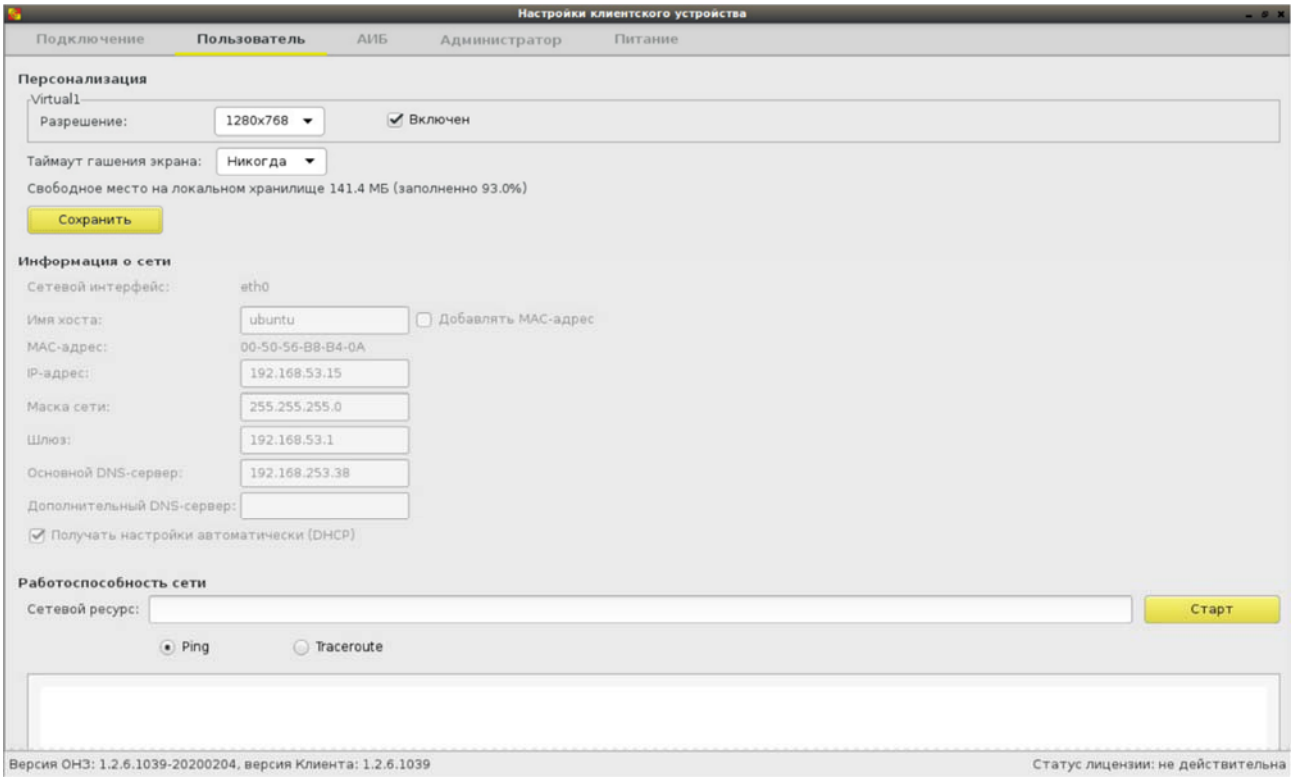

Рисунок 35 - Вкладка «Пользователь»

В разделе «Персонализация» также есть возможность изменить тайм-аут гашения экрана (по умолчанию установлен на 10 минут). Время, по истечении которого включится режим гашения экрана, можно задать в раскрывающемся списке значением из диапазона от 1 минуты до 5 часов или «Никогда».

После установки параметров мониторов и тайм-аута гашения экрана следует нажать кнопку <Сохранить>. При успешном выполнении процедуры возникает сообщение, отображенное на рисунке 36.

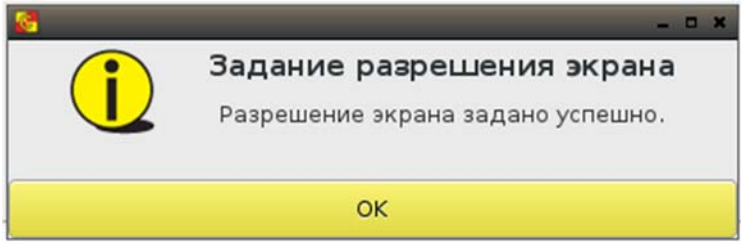

Рисунок 36 – Сообщение об успешном сохранении разрешения экрана

5.5 Просмотр сетевых настроек Клиента

Для выполнения процедуры следует перейти на вкладку «Пользователь». Здесь отображаются сетевые настройки Клиента, недоступные для изменения Пользователем.

5.6 Проверка работоспособности сетевого ресурса

Пользователь также может проводить диагностику сети. Для использования этой функции на вкладке «Пользователь» в строке «Сетевой ресурс» нужно ввести адрес ресурса, доступность которого необходимо проверить, и выбрать утилиту для проверки – «Ping» или «Traceroute», установив соответствующий флаг. Проверка начинается по кнопке <Старт>.

5.7 Настройка аудиоустройств

На вкладке «Пользователь» в разделе «Настройки аудиоустройств» (рисунок 37) есть возможность настройки устройств ввода и вывода звука.

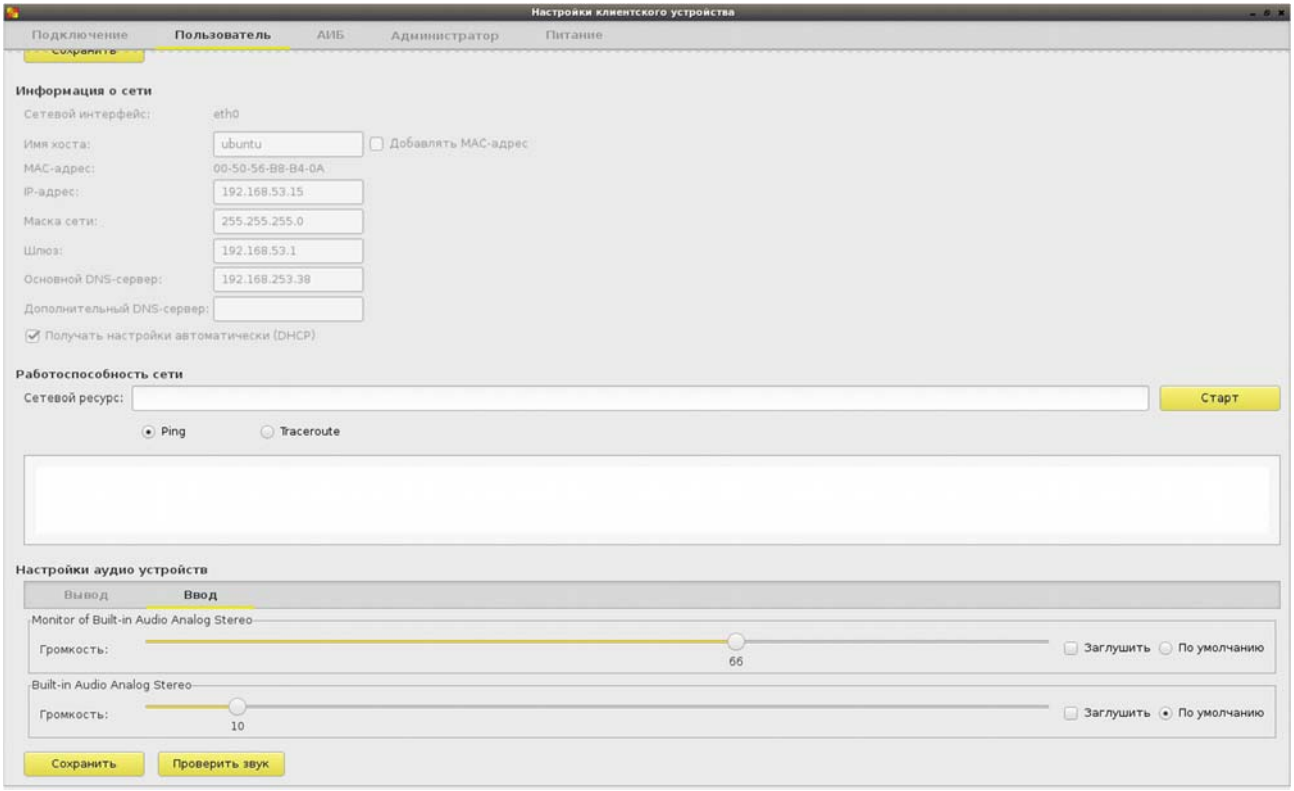

Рисунок 37 – Настройки аудиоустройств на вкладке «Пользователь»

В поле «Ввод» отображаются все устройства ввода звука (микрофоны), подключенные к терминалу пользователя, в поле «Вывод», соответственно, - устройства вывода звука (наушники, колонки и т.п.). Выбор устройства отмечается значением «По умолчанию», отключить его можно при выставлении галочки в строке «Заглушить». Для каждого устройства доступна регулировка звука, а также функция проверки звука (кнопка <Проверить звук>).

По нажатию кнопки «Проверить звук» выполняется воспроизведение тестового аудиофайла.

Для сохранения заданных настроек следует нажать кнопку <Сохранить>. При успешном сохранении появляется окно, отображенное на рисунке 38.

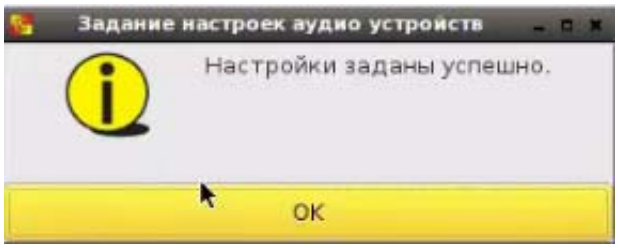

Рисунок 38 – Успешное сохранение настроек аудиоустройств

Изменения в выборе звукового устройства применяются при следующем подключении к терминальной сессии.

5.8 Настройка принтеров

В разделе «Настройка принтеров» (рисунок 39) пользователь может настроить локально подключенный к терминальной станции по USB принтер для его использования в режиме терминальной сессии.

Приведенная ниже настройка позволит также использовать принтер при работе на терминальном сервере, если клиентский образ подразумевает проброс USB, и если настройка терминального сервера[5] позволяет использовать локальные USB-принтеры. Для корректной работы локального принтера терминальный сервер также подлежит определенной настройке, которая приведена в Приложении 4.

[5] Подробнее о соответствующей настройке терминального сервера: https://support.citrix.com/article/CTX140208

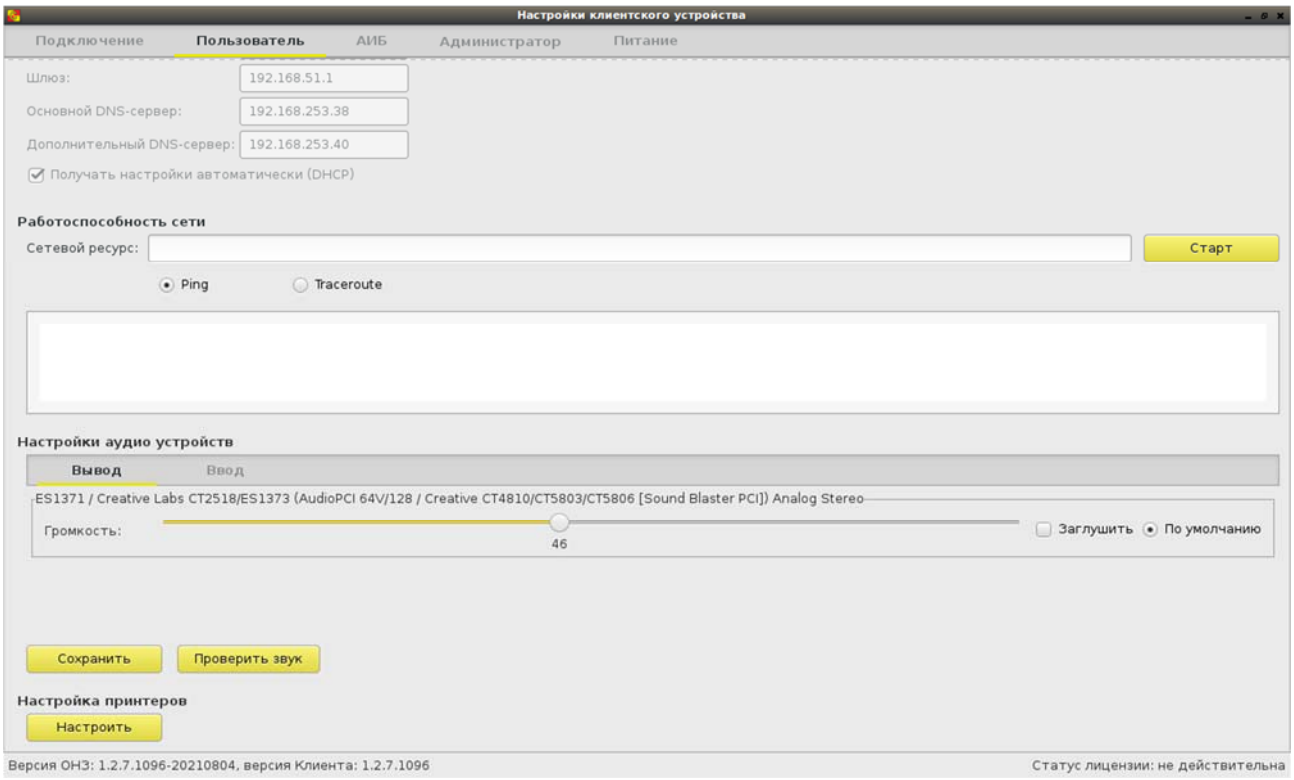

Рисунок 39 - Настройка принтеров на вкладке «Пользователь»

Окно настройки принтеров (рисунок 40) появляется при нажатии кнопки <Настроить>.

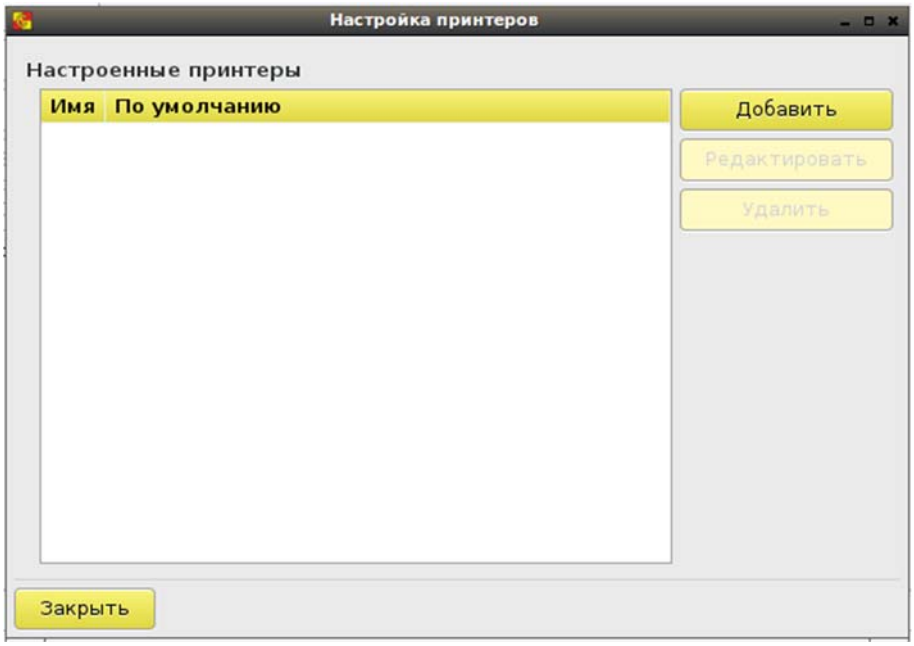

Рисунок 40 – Окно настройки принтеров

При отсутствии настроенных принтеров список пуст, и активна только кнопка <Добавить>. Прежде чем нажать на нее, следует убедиться, что настраиваемый принтер подключен к терминалу. После загрузки информации о принтере (имя и идентификатор) необходимо определить

драйверы работы с ним. Для этого следует выбрать принтер в списке и нажать кнопку <Далее> (рисунок 41).

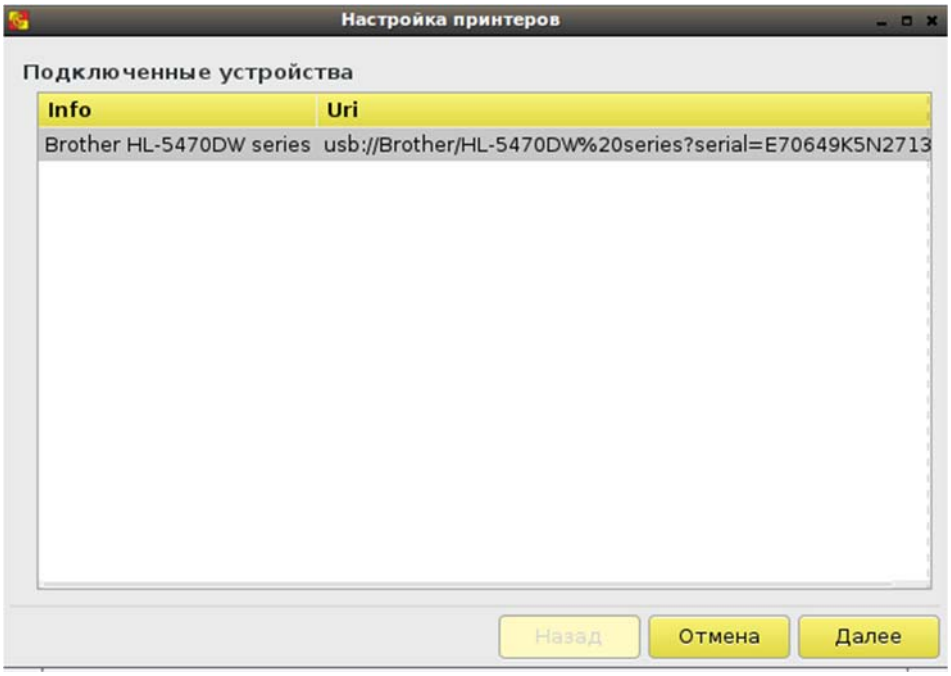

Рисунок 41 – Выбор принтера для дальнейшей настройки

В появившемся окне (рисунок 42) можно выбрать производителя принтера, а при нажатии <Далее> - в следующем окне (рисунок 43) – его модель и драйвер.

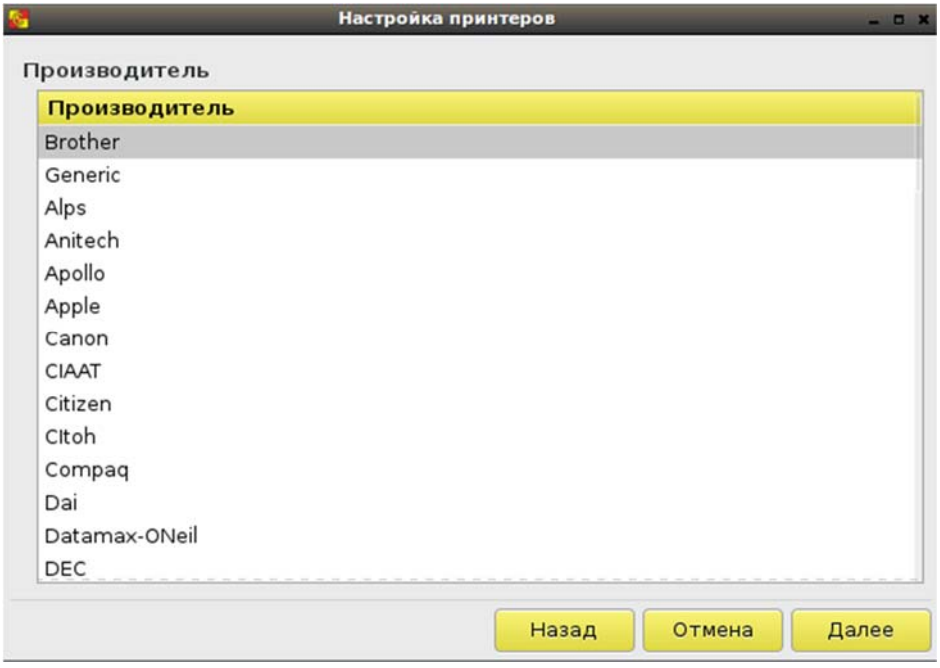

Рисунок 42 – Окно выбора производителя принтера

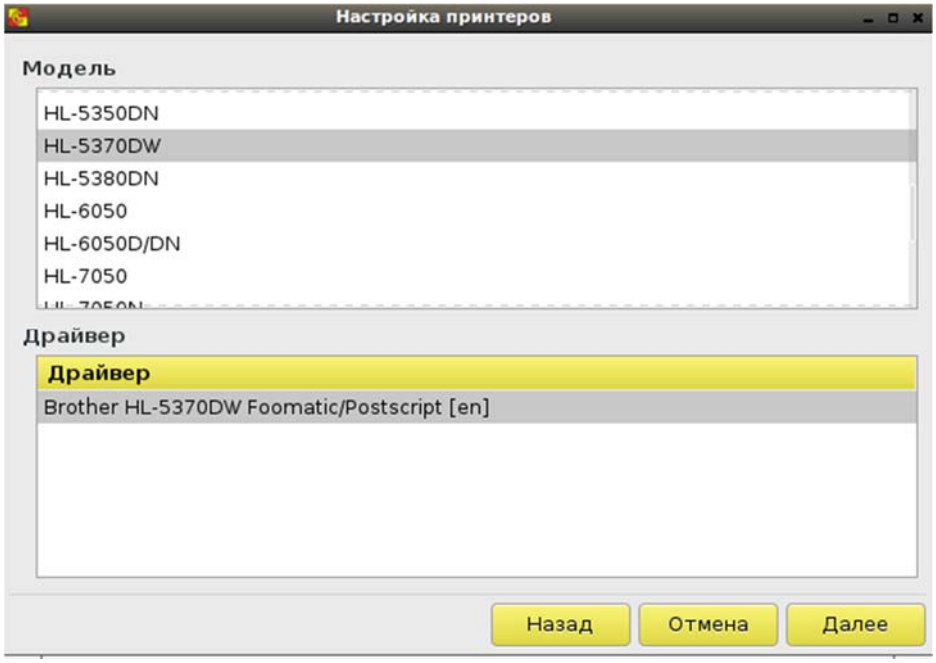

Рисунок 43 – Окно выбора модели и драйвера принтера

При отсутствии конкретной модели настраиваемого принтера можно выбрать в списке производителей универсальный принтер Generic и далее – наиболее подходящую стандартную модель. В списке драйверов для этой модели можно увидеть рекомендованный к выбору драйвер (рисунок 44).

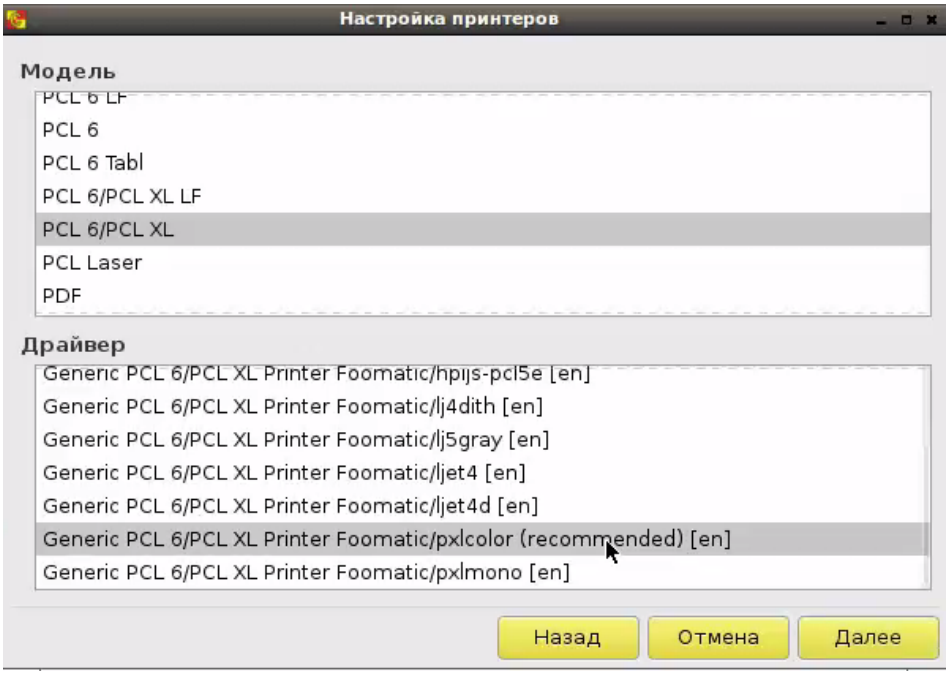

Рисунок 44 – Выбор рекомендованного драйвера для принтера Generic

После выбора драйвера при нажатии <Далее> появляется окно с общими параметрами принтера (рисунок 45), в котором можно заполнить строки «Описание», «Расположение», изменить имя принтера в одноименной строке и поставить галочку в строке «Сделать принтером по умолчанию».

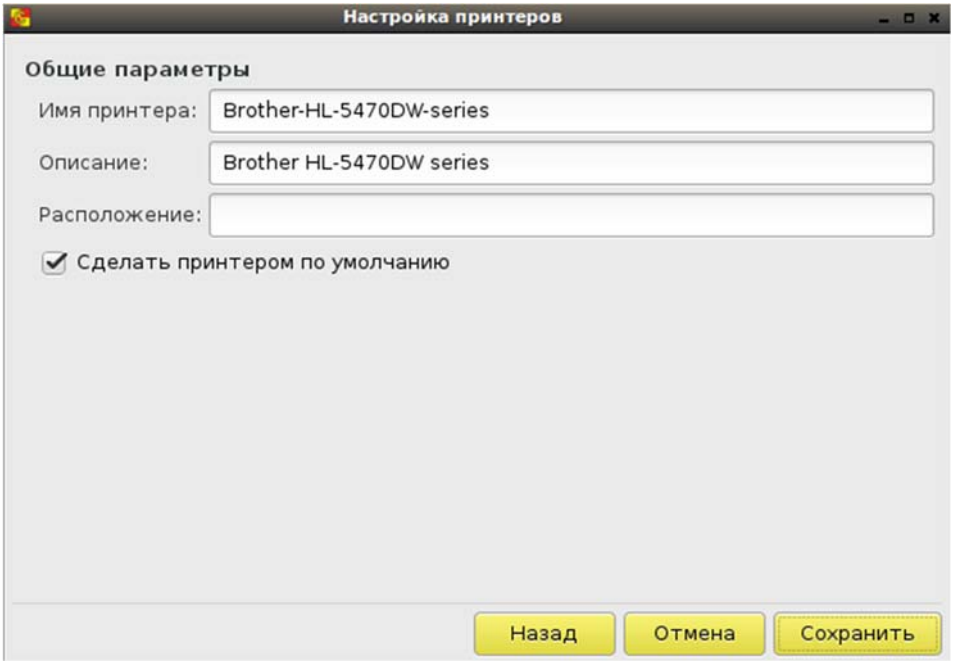

Рисунок 45 – Окно общих параметров принтера

При нажатии кнопки <Сохранить> появляется соответствующее сообщение (рисунок 46), и принтер добавляется в список настроенных (рисунок 47).

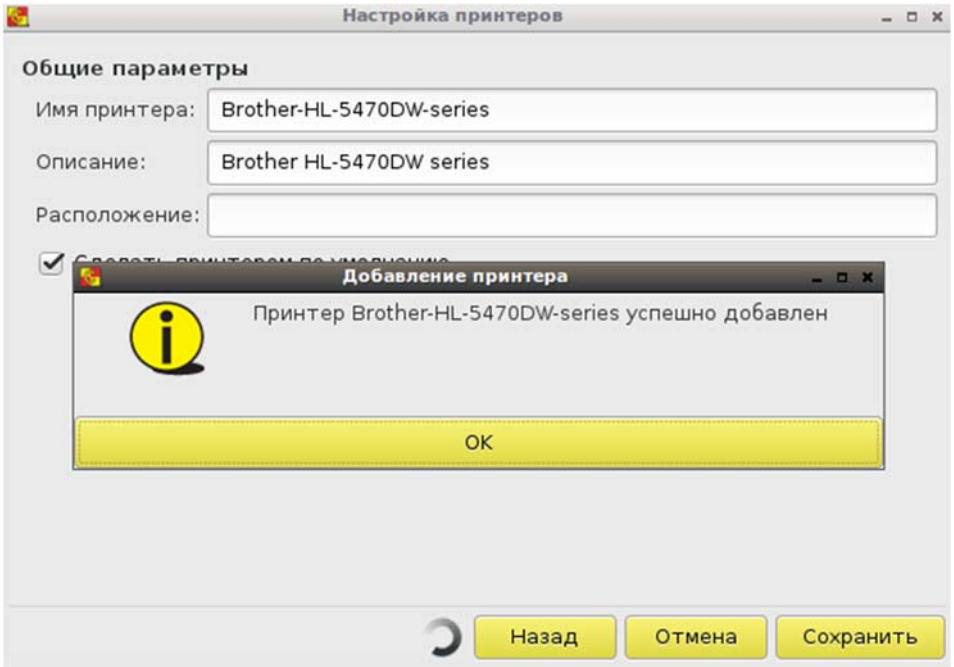

Рисунок 46 – Сообщение о добавлении принтера в список настроенных

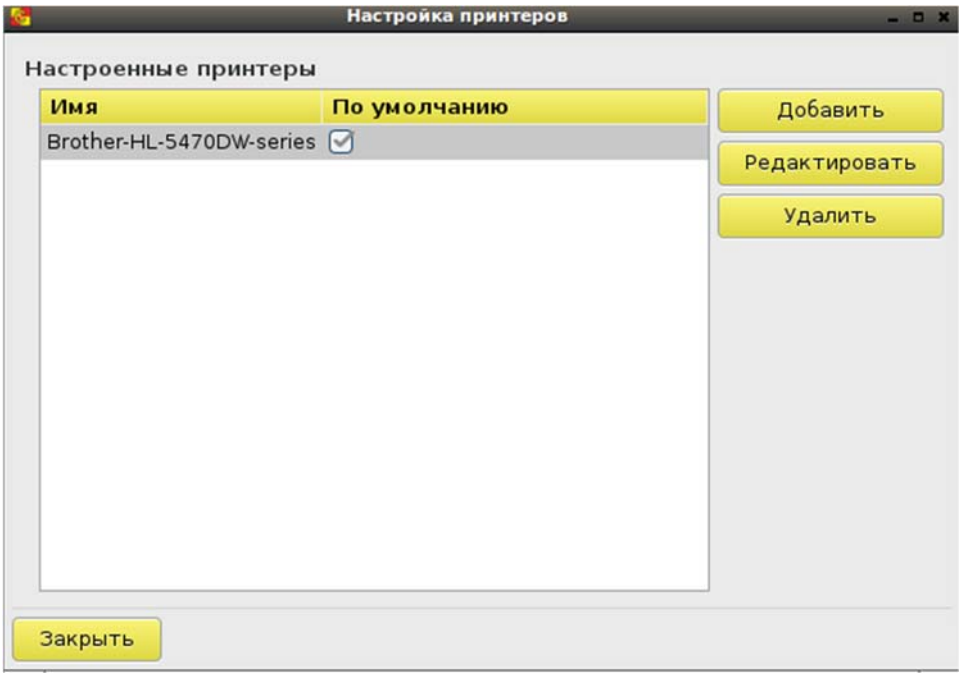

Рисунок 47 – Окно со списком настроенных принтеров

Выбрав принтер из списка настроенных, можно по кнопке <Редактировать> перейти в окно с общими параметрами и изменить описание и расположение принтера. Имя принтера и выбранный для него драйвер изменить нельзя, но можно удалить принтер из списка, подтвердив запрос на удаление (рисунок 48), и добавить принтер с другим именем.

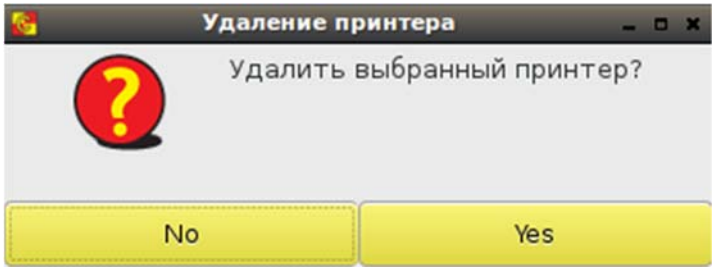

Рисунок 48 – Окно подтверждения запроса на удаление принтера

6 Завершение работы

Для завершения работы достаточно нажать кнопку питания на СВТ или использовать клавишу <F8>, свернуть окно и во вкладке «Питание» (рисунок 49) выбрать необходимое действие.

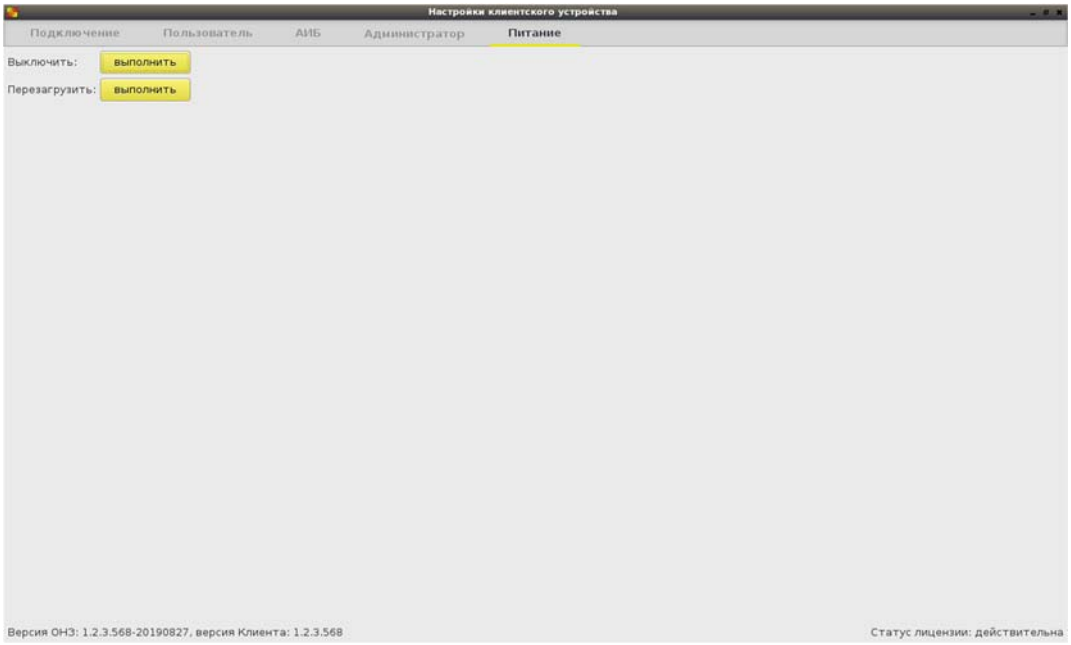

Рисунок 49 – Вкладка «Питание»

Завершить работу также можно из терминального подключения при выборе из контекстного меню, вызываемого клавишей <F8>, команды Shutdown (рисунок 33).

Следует помнить, что отключение клиентского устройства от USB-порта терминала сопровождается выключением самого терминала[6].

[6] *При использовании терминала Wyse D50D после его выключения на экране видна остаточная информация. Необходимо перед следующим его включением дополнительно выключить терминал кнопкой*

7 Перечень принятых сокращений и обозначений

БИ – безопасность информации;
ОС – операционная система;
ПАК – программно-аппаратный комплекс;
ПО – программное обеспечение;
СВТ – средство вычислительной техники;
СХСЗ – сервер хранения и сетевой загрузки;
ТС – терминальная станция.

ПРИЛОЖЕНИЕ 1.
ОСОБЕННОСТИ РАБОТЫ С ТЕРМИНАЛАМИ HP510T

При работе с терминалом HP510t возможна работа только с одним монитором. Необходимо подключать монитор к выходу DVI-I. Через DVI-D изображение не выводится.

Первый запуск Клиента

После подключения клиентского устройства к терминалу, его включения и запуска системы Пользователю следует остановить загрузку образа ПО ТС (нажать кнопку <Стоп>), перейти на вкладку «Пользователь». В разделе «Персонализация» будут отображены два монитора: VGA-1 и DVI-1.

Необходимо отключить монитор VGA-1: убрать галочку «Включен» и нажать кнопку <Сохранить>. После этого выбрать желаемое разрешение экрана из выпадающего списка для монитора DVI-1 и нажать кнопку <Сохранить>.

После этого Пользователь может приступить к работе в терминальной сессии (вкладка «Подключение», кнопка <Подключиться>).

Удаленное изменение разрешения

При удаленном задании разрешения экрана нужно учитывать следующее:

- итоговое желаемое разрешение должно выбираться для монитора DVI-1;
- разрешение для монитора VGA-1 не следует изменять.

При соблюдении этих двух условий смена разрешения экрана будет выполняться успешно.

ПРИЛОЖЕНИЕ 2
УСТАНОВКА И УДАЛЕНИЕ ПО «СПЕЦИАЛЬНЫЙ НОСИТЕЛЬ ПО ПАК ЦЕНТР-Т»

Для работы со специальными носителями ПО ПАК «Центр-Т» объемом 8ГБ в систему должно быть установлено соответствующее программное обеспечение.

Для установки ПО подключите специальный носитель с записанным на него образом ПО «Клиент Центр-Т» к АРМ с ОС Windows; устройство будет распознано системой как съемный диск (USB-накопитель).

Откройте специальный носитель (рисунок 50), зайдите в папку «SMedia» и запустите CTM_Setup_0.1.1.XX.exe (XX – номер актуальной версии устанавливаемого ПО).

ВНИМАНИЕ! Не изменяйте и не удаляйте другие файлы, так как в этом случае работоспособность специального носителя будет потеряна.

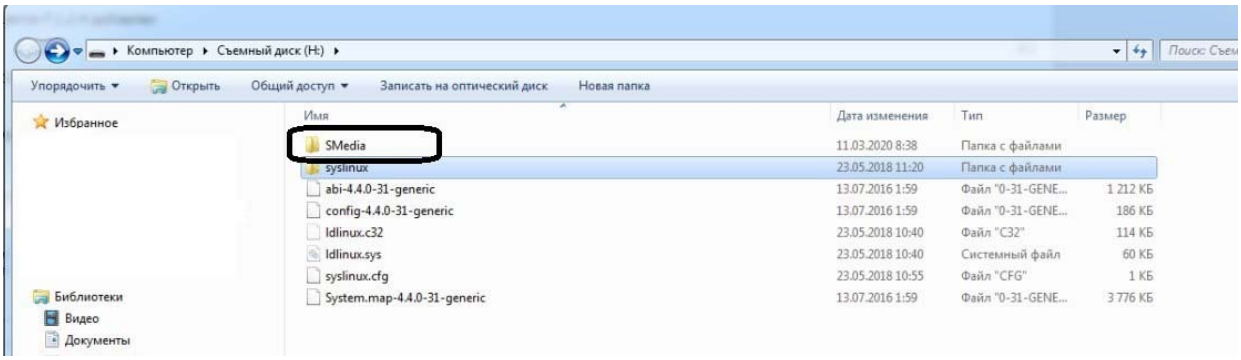

Рисунок 50 - Проводник раздела Специального носителя

После выбора языка (рисунок 51) появится мастер установки ПО (рисунок 52). Следуя его указаниям, выполните процесс установки ПО «Специальный носитель ПО ПАК Центр-Т».

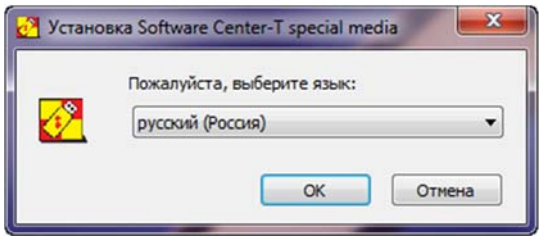

Рисунок 51 - Выбор языка установки ПО

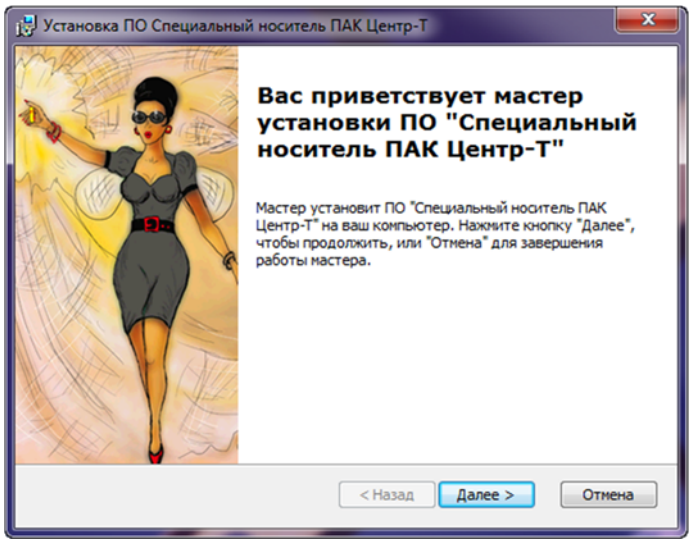

Рисунок 52 - Окно мастера установки ПО

После успешной установки ПО «Специальный носитель ПО ПАК Центр-Т» появится в списке установленных программ и компонентов (рисунок 53).

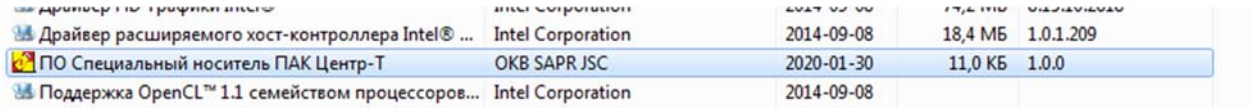

Рисунок 53 - Список установленных на компьютере программ

Удалить ПО «Специальный носитель ПО ПАК Центр-Т» можно двумя способами:

1. Через Панель управления\Программы\Программы и компоненты, нажав правой кнопкой мыши на ПО и выбрав пункт «Удалить».
2. Через повторный запуск CTM_Setup_0.1.1.XX.exe и выбор пункта «Удалить».

ПРИЛОЖЕНИЕ 3
РЕГИСТРАЦИЯ СПЕЦИАЛЬНОГО НОСИТЕЛЯ В КАЧЕСТВЕ АППАРАТНОГО ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ В ПАК «АККОРД-WIN64» («АККОРД-WIN32»)

Для регистрации специального носителя ПО ПАК «Центр-Т» в качестве идентификатора пользователя в ПАК «Аккорд-Win64» («Аккорд-Win32») необходимо установить библиотеки поддержки специального носителя в качестве аппаратного идентификатора, входящие в комплект поставки ПАК «Центр-Т» (каталог SMEDIA).

Регистрация на локальном рабочем месте

1. Выполните установку ПО «Специальный носитель ПО ПАК Центр-Т».
2. Скопируйте каталог SMEDIA в каталог Identifiers, находящийся в директории установки ПАК «Аккорд-Win64» («Аккорд-Win32»).
3. Запустите утилиту «Настройка идентификаторов Аккорд», установите в качестве дополнительного идентификатора «Специальный носитель Центр-Т 8 Гб», нажмите «Активировать».
4. Убедитесь, что при подключении специального носителя информация о нем отображается в утилитах TmExp64.exe и TmExplor.exe.
5. Зарегистрируйте специальный носитель в качестве идентификатора в утилите ACED32.

Регистрация на терминальном сервере

1. Выполните установку ПО «Специальный носитель ПО ПАК Центр-Т» на АРМ, с которого будет производиться настройка ПАК «Аккорд-Win64 TSE» («Аккорд-Win32 TSE») на терминальном сервере. Установка ПО «Специальный носитель ПО ПАК Центр-Т» на терминальный сервер не требуется.
2. Скопируйте каталог SMEDIA в каталог с установленным «Терминальным клиентом Аккорд» (Accord-TC).
3. Запустите утилиту «Настройка терминального клиента Аккорд», установите в качестве дополнительного идентификатора «Специальный носитель Центр-Т 8 Гб», нажмите «Активировать».
4. Подключитесь к терминальному серверу по протоколу ICA (откройте Citrix-сессию).
5. Убедитесь, что при подключении специального носителя информация о нем отображается на терминальном сервере в утилитах TmExp64.exe и TmExplor.exe.
6. Зарегистрируйте на терминальном сервере специальный носитель в качестве идентификатора в программе ACED32.

ПРИЛОЖЕНИЕ 4
НАСТРОЙКА ЛОКАЛЬНОГО ПРИНТЕРА НА ТЕРМИНАЛЬНОМ СЕРВЕРЕ

При использовании локального принтера в режиме терминальной сессии следует произвести определенную настройку терминального сервера, установив на нем драйвер «HP Color LaserJet 2800 Series PS (Microsoft)» (независимо от того, какой принтер на самом деле используется) в соответствии с приведенной ниже последовательностью действий.

1. В панели управления открыть вкладку «Устройства и принтеры», выбрать подключенный принтер и нажать кнопку <Свойства сервера печати> (рисунок 54).

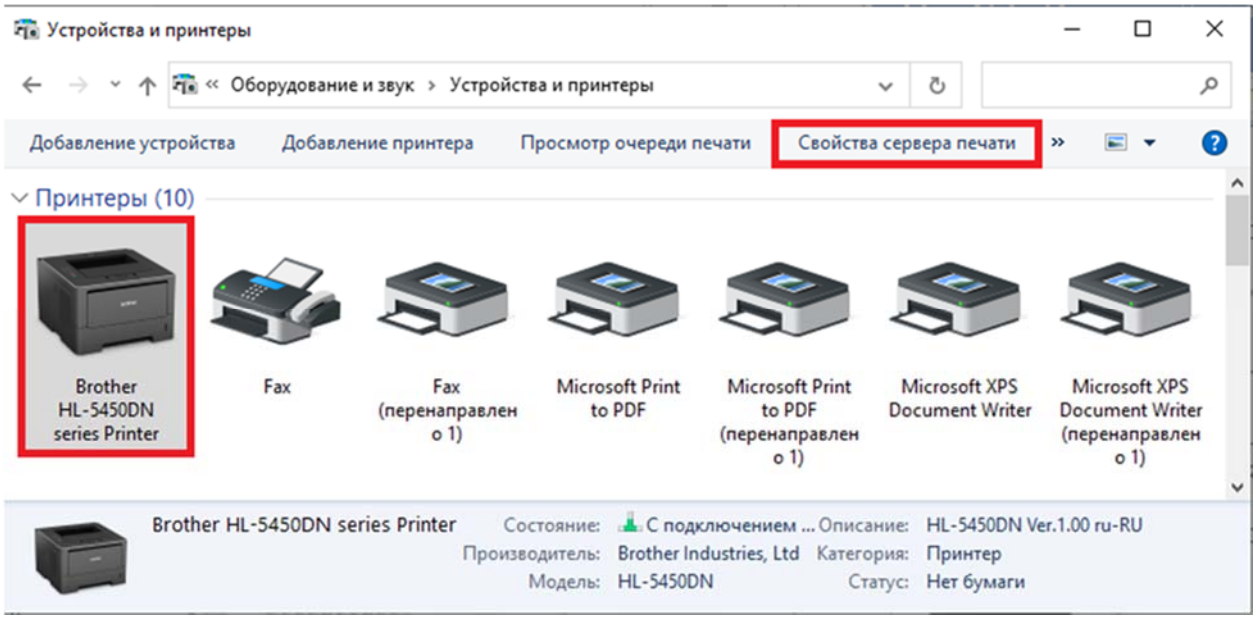

Рисунок 54 – Вкладка «Устройства и принтеры»

2. В открывшемся окне открыть вкладку «Драйверы» и нажать кнопку <Добавить> (рисунок 55).

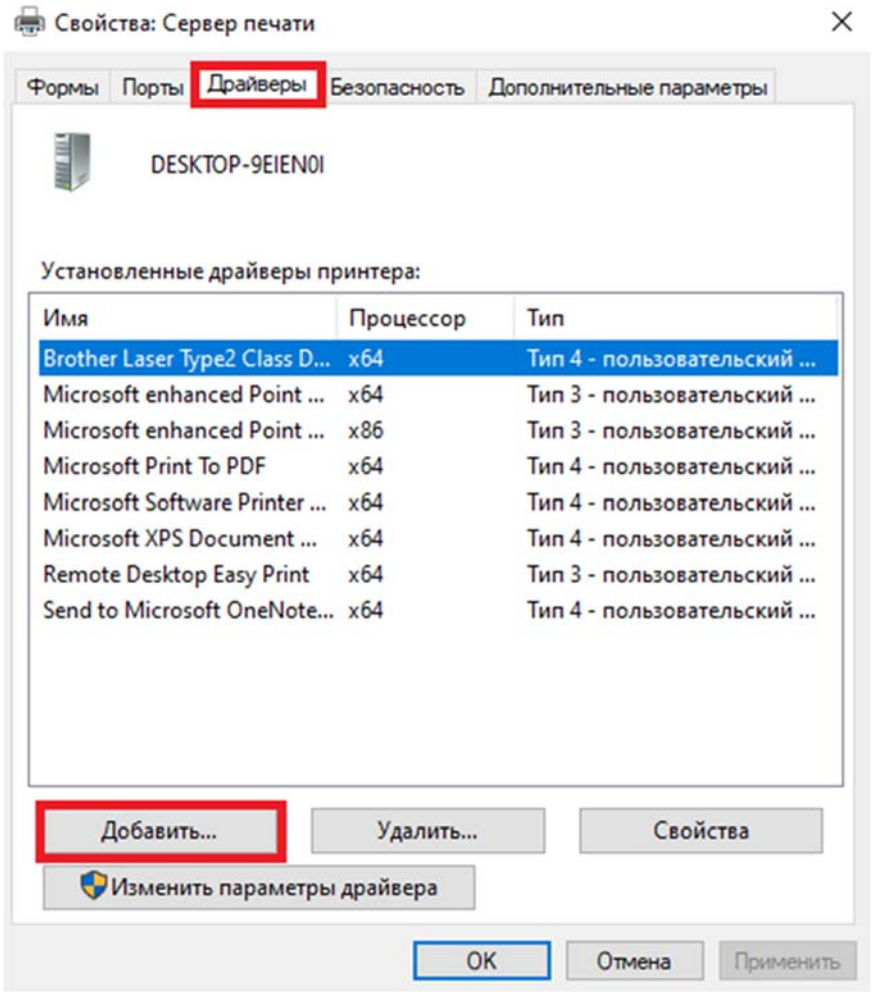

Рисунок 55 – Добавление драйвера принтера

3. В окне «Мастер установки драйверов принтера» нажать <Далее>, в следующем окне выбрать процессор (рекомендуется оставить значение, выставленное по умолчанию) и снова нажать <Далее> (рисунок 56).

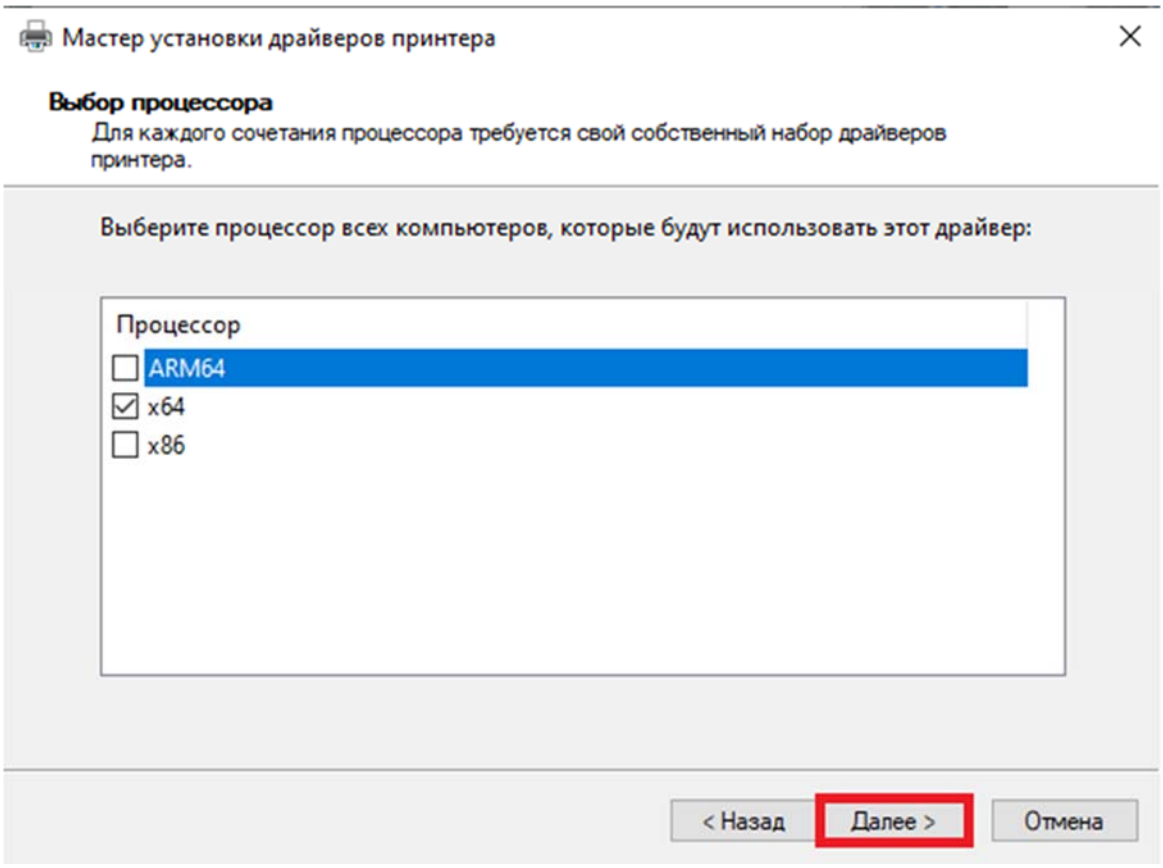

Рисунок 56 – Выбор процессора

4. В левом столбце следующего окна («Изготовитель») выбрать «HP», а в правом столбце («Принтеры») выбрать «HP Color LaserJet 2800 Series PS (Microsoft)» (рисунок 57).

ВНИМАНИЕ! Если драйвера «HP Color LaserJet 2800 Series PS (Microsoft)» нет в предложенном для выбора списке, следует нажать кнопку <Центр обновления Windows>. После того как Windows обновит список принтеров, драйвер «HP Color LaserJet 2800 Series PS (Microsoft)» появится в колонке «Принтеры» и будет доступен для выбора.

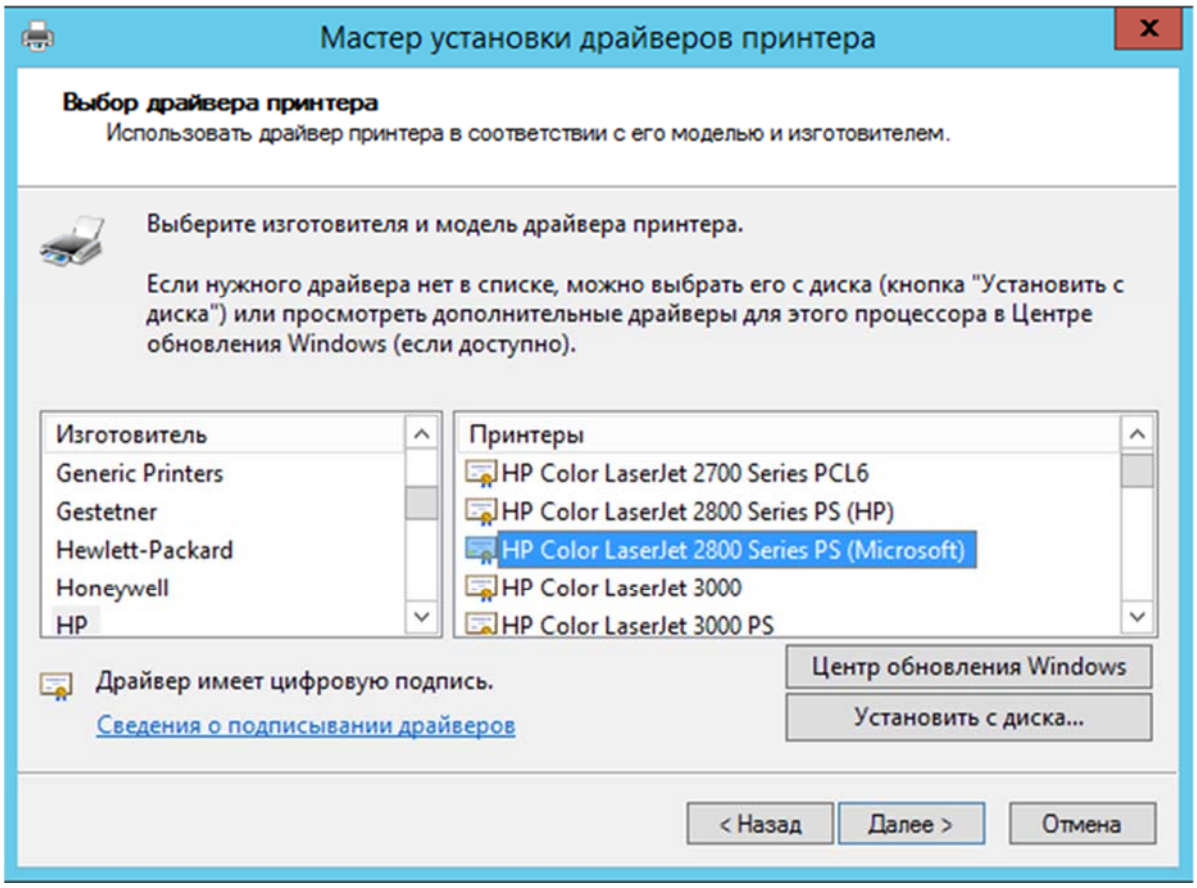

Рисунок 57 – Выбор драйвера принтера

5. Нажать «Далее» и (в следующем окне) <Готово> для завершения установки.

ПРИЛОЖЕНИЕ 5
ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ В КАЧЕСТВЕ ТЕРМИНАЛЬНОЙ СТАНЦИИ ЗАЩИЩЕННОГО ТЕРМИНАЛА ЦЕНТР-TRUST

В случае использования в качестве терминальной станции Защищенного терминала Центр-TrusT загрузка специального ОНЗ, аналогичного ОНЗ, записываемому на носитель ПО «Клиент», осуществляется с диска терминала.

После загрузки запущенное ПО Клиента ожидает подключения к Защищенному терминалу Центр-TrusT клиентского устройства (рисунок 58).

Рисунок 58 – Запрос на подключение носителя ПО Клиента

После подключения клиентского устройства выполняется считывание с него локальных настроек Клиента, влияющих на работу ПАК «Центр-Т» на Защищенном терминале: пин-кодов Администратора и Администратора БИ клиентского устройства, настройки RMQ и репозитория образов, а также записи журнала о локальных событиях безопасности. Настройки, влияющие на работу терминальной станции (сетевые настройки и настройки времени, разрешение экрана и тайм-аут его гашения, а также настройки аудиоустройств), хранятся на диске Защищенного терминала, и ПО Клиента считывает их с диска.

После получения всех настроек ПО Клиента начинает работу в штатном режиме.

Работа Пользователя, Администратора и Администратора БИ клиентского устройства соответствует описанию, приведенному в разделах 3-5 данного руководства.

При завершении работы штатным образом (через вкладку «Питание» ПО Клиента) измененные настройки RMQ и репозитория образов (если они были изменены во время работы), а также новые записи журнала о локальных событиях безопасности копируются на клиентское устройство, а Защищенный терминал Центр-TrusT завершает свою работу. После этого клиентское устройство может быть извлечено.