ОКБ САПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

(Версия 1.3.0)

Руководство по эксплуатации СХСЗ

37222406.26.20.40.140.042 91

Листов 123

Москва

2023

АННОТАЦИЯ

Настоящий документ является руководством по управлению механизмами Сервера хранения и сетевой загрузки (СХСЗ) программного обеспечения (ПО) терминальных станций (ТС) из состава программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Центр-Т» (далее – ПАК «Центр-Т», Комплекс) и предназначен для должностных лиц, выполняющих роли Администратора безопасности информации СХСЗ, Администратора СХСЗ, Контролера эксплуатации, Администратора нештатного режима и Администратора сервисного режима работы СХСЗ.

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.

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

СХСЗ – это автоматизированное рабочее место, предназначенное для сетевой загрузки ПО ТС.

Специализированное ПО СХСЗ хранится и загружается из памяти носителя.

Схема работы выглядит следующим образом:

с носителя ПО СХСЗ стартует ПО СХСЗ. На момент начала эксплуатации оно содержит предварительно подготовленные образы операционной системы (ОС) Linux, содержащие необходимое ПО для соединения с терминальным сервером;

с носителя ПО Клиента (далее также – клиентское устройство) стартует образ начальной загрузки (ОНЗ), также реализованный на основе ОС Linux;

на СХСЗ посылается запрос на получение образа ПО ТС;

СХСЗ обрабатывает запрос и выдает клиенту нужный образ ПО ТС;

клиентское устройство принимает образ по сети и проверяет его. Если проверка завершается успешно, то он загружается в оперативную память СВТ и ему передается дальнейшее управление ресурсами компьютера;

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

Функции СХСЗ в системе терминального доступа следующие:

1) управление учетными записями пользователей;
2) управление образами и шаблонами настроек образов ПО ТС;
3) предоставление образов клиентам (загрузка по сети).

Функции управления СХСЗ разделены между пятью административными ролями: Администратором сервисного режима, Администратором СХСЗ (далее – Администратор), Администратором БИ СХСЗ (далее – Администратор БИ), Контролером эксплуатации (далее - Контролер) и Администратором нештатного режима (далее – Администратор НШР). Функции указанных ролей 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 разработанные учетные и объектовые 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.

Также обратите внимание на минимальные и рекомендуемые технические характеристики СХСЗ в зависимости от возможного количества одновременно запускаемых клиентов:

- для 50 клиентов минимальные - 1CPU, 1Gb, рекомендуемые - 2CPU, 2Gb;
- для 75 клиентов минимальные - 2 CPU, 2Gb, рекомендуемые - 4CPU, 8Gb.

Начиная с версии 1.2.10 в комплект поставки ПАК «Центр-Т» входит образ диска vmdk для создания виртуального СХСЗ. Технические характеристики виртуальной машины, создаваемой для использования в качестве СХСЗ, должны удовлетворять отмеченным выше.

1. Объем работы администраторов СХСЗ

Основными процедурами, выполняемыми администраторами СХСЗ, являются:

- планирование применения СХСЗ;
- смена PIN-кода Администратора сервисного режима;
- установка сетевых настроек СХСЗ;
- копирование лицензии на СХСЗ;
- смена пароля и аппаратного идентификатора Администратора и Администратора БИ;
- создание/удаление/редактирование/экспорт учетных записей;
- назначение роли учетным записям;
- управление образами ПО ТС (просмотр/удаление образов);
- управление шаблонами настроек образов ПО ТС (создание/редактирование/удаление);
- назначение пользователям клиентских устройств;
- назначение пользователям образов ПО ТС;
- назначение пользователям шаблонов настроек образа;
- работа с журналами регистрации действий пользователей и администраторов;
- резервирование и восстановление СХСЗ;
- настройка даты и времени СХСЗ;
- настройка разрешения экрана СХСЗ;
- настройка тайм-аута гашения экрана СХСЗ;
- просмотр информации об используемом Клиентами оборудовании;
- просмотр состояния контейнеров;
- управление завершением работы СХСЗ;
- управление отладочным режимом.

Планирование применения СХСЗ осуществляется всеми администраторами СХСЗ, процедуры планирования описаны в разделе 2.

Администратор сервисного режима работы СХСЗ производит:

- смену PIN-кода Администратора сервисного режима работы СХСЗ;
- установку сетевых настроек СХСЗ;
- проверку работоспособности сети;
- настройки брокера сообщений RMQ и базы данных (БД);

– подключение внешнего носителя для резервирования и восстановления БД СХСЗ;

– копирование лицензии на СХСЗ;

– резервирование и восстановление СХСЗ;

– настройку даты и времени, а также синхронизацию с NTP-сервером;

– настройку разрешения и тайм-аута гашения экрана СХСЗ;

– просмотр информации об используемом Клиентами оборудовании;

– просмотр журнала событий собственной сессии и контейнеров;

– просмотр состояния контейнеров;

– управление завершением работы СХСЗ;

– управление отладочным режимом.

Администратор сервисного режима работы СХСЗ выполняет свои функции локально в ПО сервисного режима.

Администратор производит:

– смену пароля и аппаратного идентификатора Администратора;

– просмотр журнала событий собственной сессии;

– создание, удаление, редактирование, экспорт учетных записей;

– управление шаблонами настроек образов ПО ТС;

– редактирование настроек пользователя (разрешение и тайм-аута гашения экрана, настройки аудиоустройств и кеширование образов);

– просмотр информации об используемом Клиентами оборудовании;

– просмотр журналов регистрации действий пользователей и администраторов.

Администратор БИ выполняет следующие процедуры:

– смену пароля и аппаратного идентификатора Администратора БИ;

– просмотр журнала событий собственной сессии;

– назначение роли учетным записям;

– экспорт учетных записей;

– управление образами ПО ТС;

– просмотр шаблонов настроек образов ПО ТС;

– назначение пользователям клиентских устройств;

– назначение пользователям образов ПО ТС;

– назначение пользователям шаблонов образов ПО ТС;

– редактирование настроек пользователя (кроме разрешения экрана и кеширования образов);

– просмотр информации об используемом Клиентами оборудовании;

– просмотр журналов регистрации действий пользователей и администраторов.

Контролер выполняет следующие процедуры:

– смену пароля и аппаратного идентификатора Контролера;

– просмотр журнала событий собственной сессии;

– просмотр образов ПО ТС;

– просмотр шаблонов настроек образов ПО ТС;

– просмотр настроек пользователя;

– экспорт учетных записей;

– просмотр информации об используемом Клиентами оборудовании;

– просмотр журналов регистрации действий пользователей и администраторов.

Администратор НШР выполняет следующие процедуры:

– смену пароля и аппаратного идентификатора Администратора НШР;

– просмотр журнала событий собственной сессии;

– создание, удаление, редактирование, экспорт учетных записей;

– управление образами ПО ТС;

– управление шаблонами настроек образов ПО ТС;

– назначение пользователям клиентских устройств;

– назначение пользователям образов ПО ТС;

– назначение пользователям шаблонов образов ПО ТС;

– редактирование настроек пользователя (разрешение и таймаута гашения экрана, настройки аудиоустройств и кеширование образов);

– просмотр информации об используемом Клиентами оборудовании;

– просмотр журналов регистрации действий пользователей и администраторов.

Администратор, Администратор БИ, Администратор НШР и Контролер СХСЗ (далее также – администраторы удаленного управления СХСЗ) выполняют свои функции в ПО управления СХСЗ удаленно с собственных рабочих мест.

По умолчанию созданы только две учетные записи: Администратора (admin) и Администратора БИ (aib). Создание учетных записей Администратора НШР и Контролера производится в процессе эксплуатации Комплекса при необходимости.

2. Планирование применения СХСЗ

Планирование применения ПАК «Центр-Т» осуществляется с учетом общей политики обеспечения безопасности в организации (на предприятии, фирме и т.д.).

Для настройки и эксплуатации СХСЗ в соответствии с перечнем выполняемых действий:

- Администратор сервисного режима должен получить:
  - носитель ПО СХСЗ с образами ПО ТС;
  - информацию для настройки сети СХСЗ (IP-адрес, маску сети, шлюз, DNS).
- Администратор должен получить списки пользователей СВТ.
- Администратор БИ должен получить:
  - списки серийных номеров клиентских устройств;
  - журнал, в котором серийные номера клиентских устройств соотнесены с ФИО пользователей;
  - перечень серверов, с которыми будут взаимодействовать пользователи (IP-адреса, маски сети, шлюз и т.д.);
  - документ, описывающий порядок и правила предоставления, изменения и утверждения конкретным должностным лицом необходимых полномочий по доступу к ресурсам СВТ;
  - документ, описывающий порядок и периодичность анализа системных журналов регистрации и принятия мер по зарегистрированным несанкционированным действиям пользователей СВТ.

Для создания каждому пользователю изолированной программной среды необходимо, чтобы вышеназванные документы 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.

3. Состав работ Администратора сервисного режима

3.1. Общие сведения

При получении носителя ПО СХСЗ Администратор сервисного режима:

1) организует загрузку сервера, который планируется использовать в качестве СХСЗ, с носителя ПО СХСЗ;

2) получает доступ к ПО сервисного режима (см. 3.2);

3) устанавливает PIN-код Администратора сервисного режима в принудительном порядке (см. 3.2);

4) копирует лицензию (при необходимости) (см. 3.3);

5) устанавливает сетевые настройки СХСЗ (см. 3.4).

Примечание: *Если в системе предусмотрено АРМ ЗХСЗ, настройки СХСЗ может устанавливать администратор АРМ ЗХСЗ (подробнее см. Руководство по эксплуатации АРМ ЗХСЗ 37222406.26.20.40.140.042 92).*

В процессе эксплуатации СХСЗ Администратор сервисного режима должен запускать СХСЗ в начале рабочего дня (если регламентирующими документами организации предписано выключение СХСЗ на ночь). Также в процессе эксплуатации ему доступны:

1) управление отладочным режимом (см. 3.4);

2) управление сетевыми настройками (см. 3.4);

3) задание разрешения и тайм-аута гашения экрана СХСЗ (см. 3.4);

4) настройка подключения к брокеру сообщений RabbitMQ и базе данных (см. 3.4);

5) резервирование и восстановление базы данных СХСЗ (см. 3.5);

6) настройка даты и времени, в том числе синхронизации с NTP-сервером (см. 3.6);

7) мониторинг состояния контейнеров (см. 3.7);

8) смена собственного PIN-кода (см. 3.8);

9) работа с журналами регистрации событий (см. 3.9, 3.10);

10) управление завершением работы СХСЗ (см.3.11);

11) организация работы при наличии в системе терминального доступа СХСЗ ПАК «Центр-Т» версии 1.1.8.

Если загрузка СХСЗ выполняется на сервере HP с поддержкой интерфейса удаленного управления iLO, администратор сервисного режима при использовании функций Remote Console может выполнять удаленную настройку СХСЗ с учетом особенностей, описанных в п. 3.5.2 и 6.3.

3.2. Получение доступа к ПО сервисного режима

При загрузке СВТ с носителя происходит подготовка старта ПО.

Далее выполняется загрузка ПО сервисного режима работы СХСЗ.

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

Обратите внимание, что в случае использования СХСЗ на базе защищенного микрокомпьютера ПО сервисного режима имеет желто-черный графический интерфейс.

Рисунок 1 – Окно установки PIN-кода Администратора сервисного режима при первом запуске

В изображенном на рисунке 1 окне нужно ввести PIN-код с подтверждением и нажать кнопку <Сохранить> (<Enter>). В результате успешной установки PIN-кода появляется оповещение, отраженное на рисунке 2.

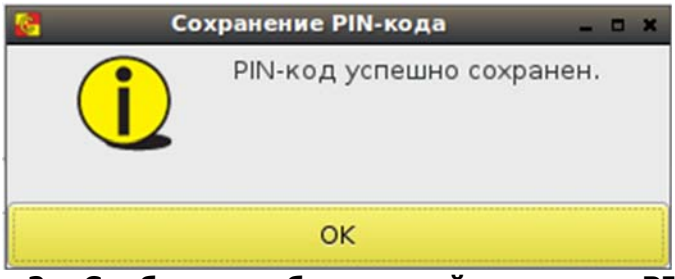


Рисунок 2 – Сообщение об успешной установке PIN-кода

Для продолжения работы следует закрыть информационное окно.

Если PIN-код уже установлен, после загрузки ПО СХСЗ появляется окно идентификации Администратора сервисного режима.

В случае ввода корректного PIN-кода появляется главное окно ПО сервисного режима.

При небольшом разрешении экрана имеющиеся вкладки отображаются не полностью и доступны после прокрутки.

3.3. Копирование лицензии

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

В случае если запись образа СХСЗ на носитель производилась администратором сервисного режима, в начале работы необходимо перенести на СХСЗ файл лицензии. Для этого предварительно файл лицензии должен быть скопирован на внешний USB-носитель, который в дальнейшем подключается к СХСЗ.

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 копируется лицензия. Монтирование внешнего носителя осуществляется на вкладке «USB Носитель» (рисунок 3).

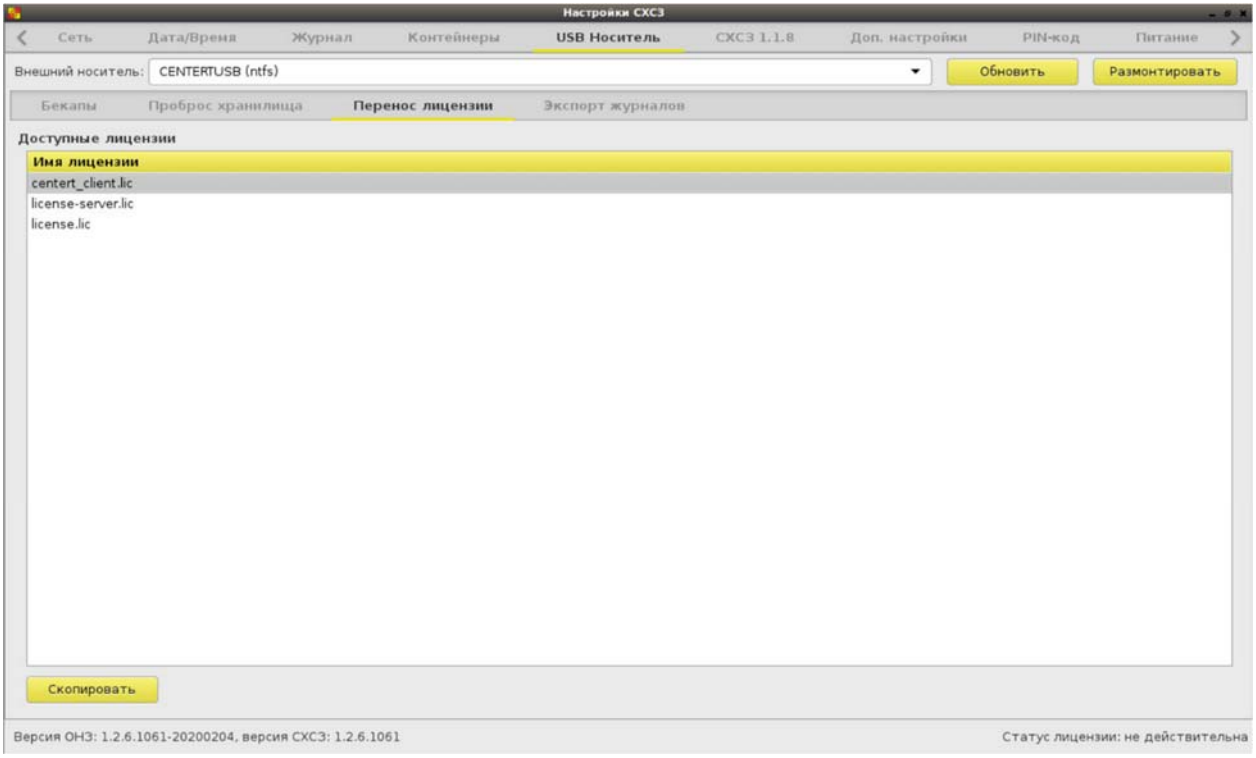


Рисунок 3 - Монтирование внешнего носителя для переноса на него лицензии

После подключения внешнего носителя к разъему СХСЗ следует нажать кнопку <Обновить> (F5), выбрать его имя в строке «Внешний носитель», выбрать пункт «Перенос лицензии» и нажать кнопку <Монтировать>. После этого в поле «Имя лицензии» будут отображены все файлы лицензий из каталога «lic» внешнего носителя (рисунок 3).

После выбора лицензии из списка станет активной кнопка «Копировать на устройство», при нажатии на которую произойдет перенос файла на СХСЗ и появится информационное сообщение о копировании (рисунок 4).

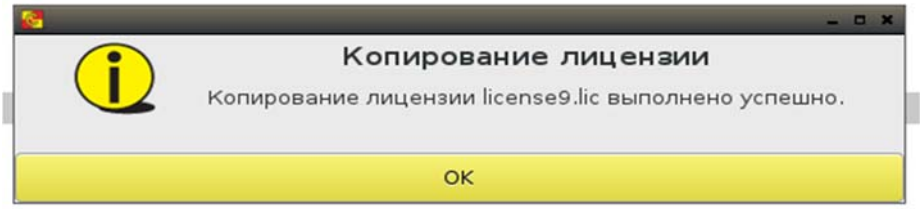


Рисунок 4 - Сообщение об успешном копировании лицензии

Далее следует выйти из утилиты удаленного администрирования СХСЗ и снова запустить ее.

Проверить, что лицензия успешно скопирована и действительная, можно одним из следующих способов:

1) через просмотр событий «Сервиса управления» во вкладке «Журналы» (подробнее см. раздел 3.9).
2) через утилиту удаленного администрирования СХСЗ: администраторы удаленного режима во вкладке «О продукте» имеют возможность просмотреть информацию о лицензии (подробнее – раздел 4.11).

Если файл лицензии не был скопирован, или он поврежден, или недействителен по какой-либо другой причине, будет выдано соответствующее информационное сообщение (рисунки 5-7) с отражением в журнале «Сервиса управления» и в утилите удаленного администрирования СХСЗ.

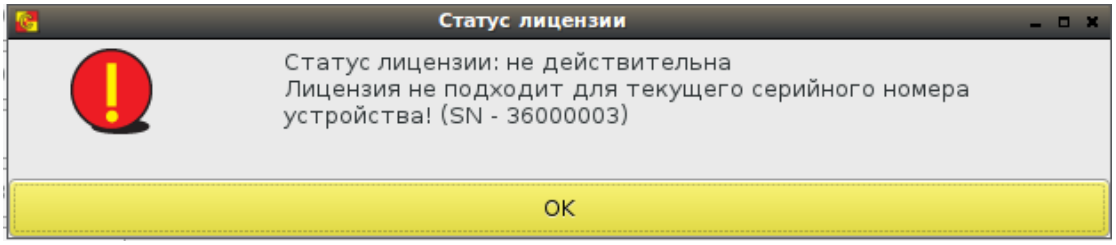


Рисунок 5 - Ошибка копирования лицензии для носителя с другим серийным номером (в скобках указан номер подключенного носителя)

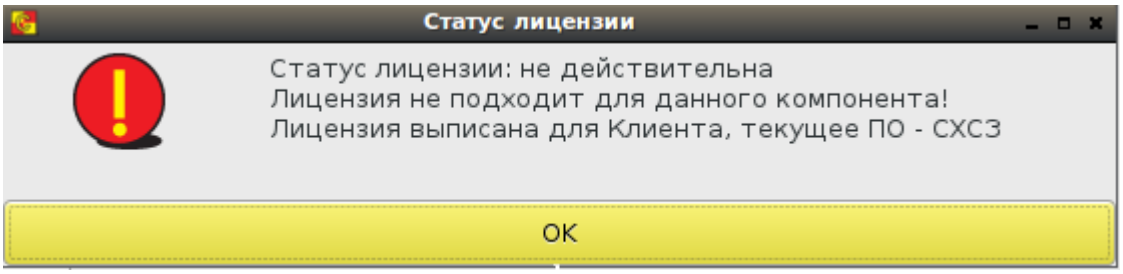


Рисунок 6 – Ошибка копирования лицензии для носителя ПО Клиента

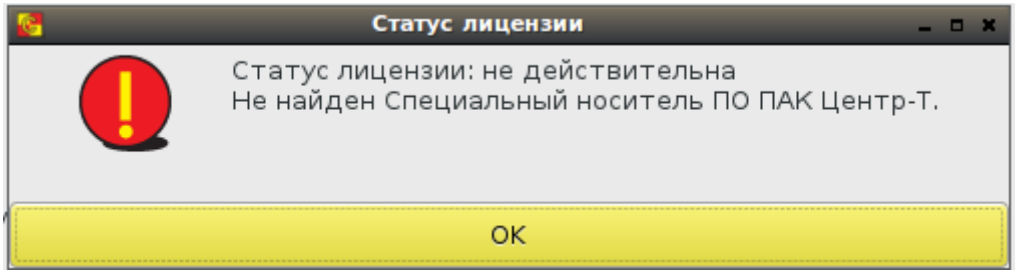


Рисунок 7 – Ошибка копирования лицензии для неподключенного носителя при переносе лицензии на виртуальный СХСЗ[1]

При изменении лицензии обновленные данные появятся в утилите удаленного управления СХСЗ при следующем подключении.

3.4. Установка разрешения и тайм-аута гашения экрана и сетевых настроек

Настройка разрешения экрана СХСЗ выполняется на вкладке «Сеть» ПО сервисного режима работы (рисунок 8) в разделе «Персонализация». Для настройки необходимо выбрать из выпадающего списка нужное значение разрешения, после чего нажать кнопку <Сохранить>.

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».

В случае успешной установки настроек возникает сообщение, отображенное на рисунке 9.

[1] Возможность создания виртуального СХСЗ появилась в ПАК «Центр-Т» версии 1.2.11. Его работа обеспечивается только при постоянно подключенном Специальном носителе ПО ПАК «Центр-Т»

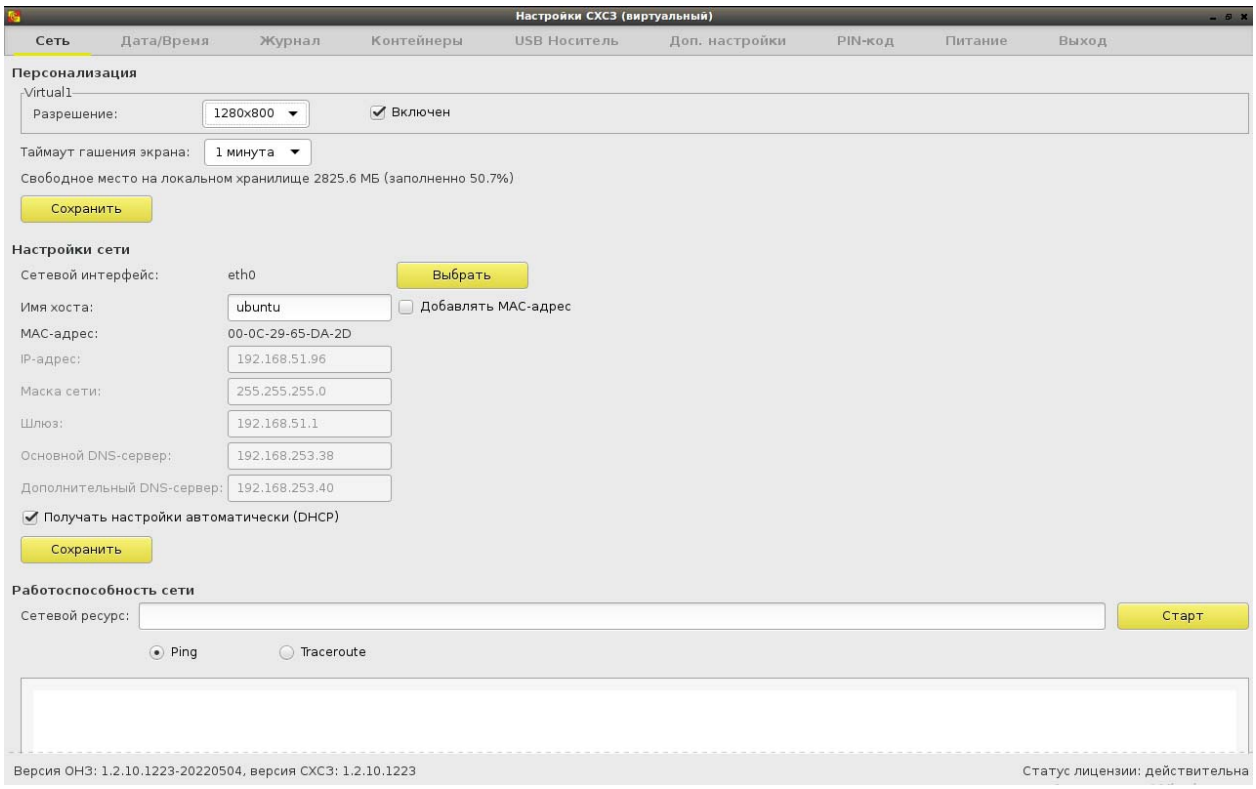


Рисунок 8 – Вкладка «Сеть»[2]

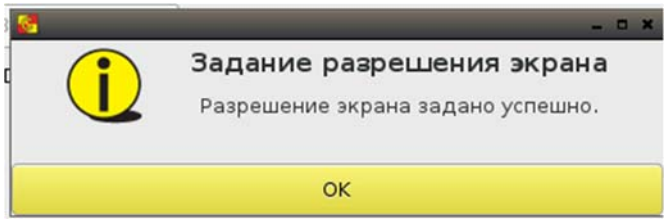


Рисунок 9 - Сообщение об успешной установке разрешения экрана

Сетевые настройки, необходимые для функционирования СХСЗ, включают в себя:

- общие сетевые настройки СХСЗ;
- сетевые настройки используемых внешних ресурсов.

Установка общих сетевых настроек СХСЗ выполняется на вкладке «Сеть» ПО сервисного режима работы (рисунок 8).

Доступны следующие сетевые настройки:

– «Сетевой интерфейс» - позволяет задать имя используемого сетевого интерфейса. Выбор интерфейса происходит при запуске ПО СХСЗ. Если при более раннем запуске ПО интерфейс уже был выбран, в строке отобразится его ранее установленное имя. Если в системе будет обнаружен единственный интерфейс стандартного типа (eth0, eth1 и т.п.), то это имя и будет отображено. В остальных случаях при старте приложения «Настройки СХСЗ» появится окно выбора интерфейса, в

[2] В названии окна отражен статус СХСЗ - виртуальный (начиная с версии 1.2.10)

котором будет предложено выбрать сетевой интерфейс из выпадающего списка с доступными именами (рисунок 10). При нажатии кнопки <Выбрать> выбор будет подтвержден (рисунок 11), если окно закрыть, не сделав выбора, то при загрузке приложения в строке «Сетевой интерфейс» появится значение «не выбран». В этом случае окно выбора интерфейса (рисунок 10) доступно по кнопке <Выбрать> в правой части строки (рисунок 8). Если выбор не сделать, то при каждом переключении между вкладками окна «Настройки СХСЗ» или при обновлении (F5) будет появляться окно напоминания (рисунок 12).

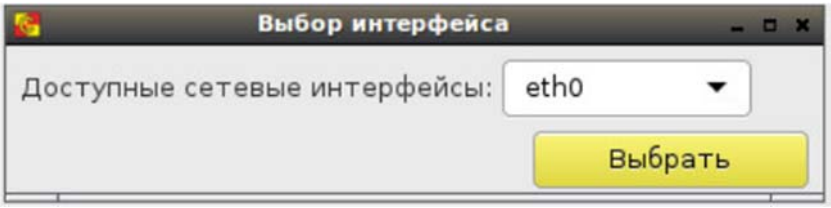


Рисунок 10 - Окно выбора сетевого интерфейса

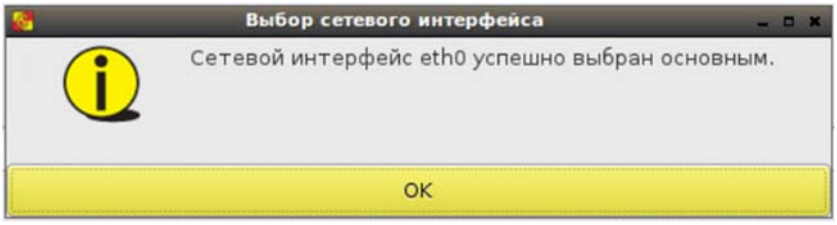


Рисунок 11 - Окно подтверждения выбора сетевого интерфейса

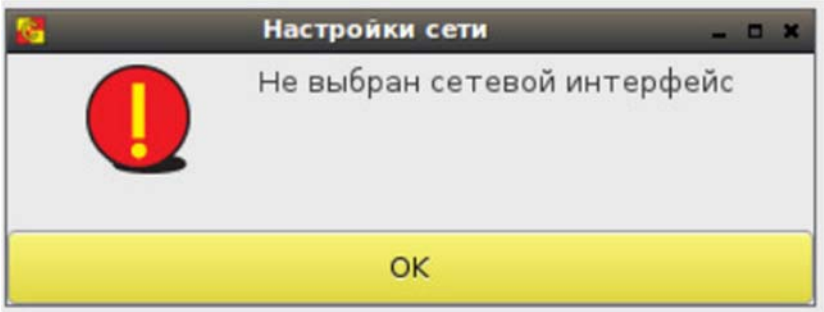


Рисунок 12 - Напоминание о том, что сетевой интерфейс не выбран

– «Получать настройки автоматически (DHCP)» – позволяет включить/выключить функцию получения сетевых настроек СХСЗ 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 (включая первый запуск) флаг установлен;

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

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

– «Шлюз» – позволяет задать шлюз подсети СХСЗ;

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

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

После установки требуемых значений следует нажать кнопку <Сохранить>. В случае успешной установки настроек возникает сообщение, отображенное на рисунке 13.

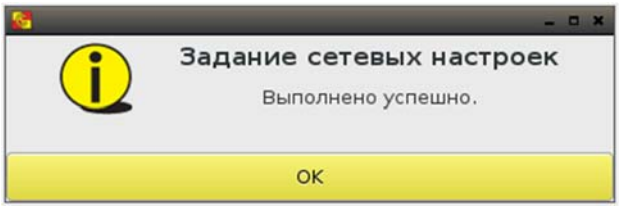


Рисунок 13 – Сообщение об успешной установке сетевых настроек

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

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

Установка сетевых настроек используемых внешних ресурсов по умолчанию не требуется (достаточно ресурсов, которые есть на самом СХСЗ).

В случае необходимости допускается переход на внешний брокер сообщений - сервер RabbitMQ[3] и в базу данных (БД) PostgreSQL. Это выполняется на вкладке «Доп. настройки» (рисунок 14).

[3] В Приложении 6 приведена инструкция по изменению базовой директории RabbitMQ

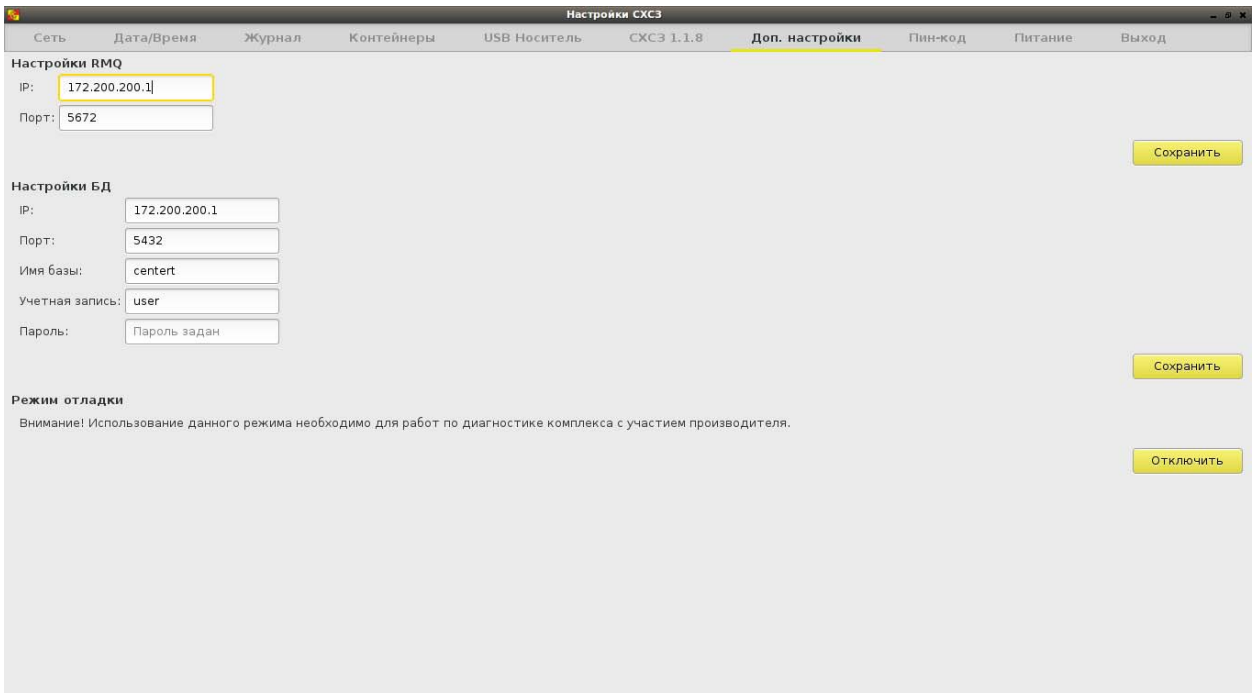


Рисунок 14 – Вкладка «Доп. настройки»

Для настройки брокера сообщений Администратору сервисного режима работы необходимо задать IP-адрес и порт в разделе «Настройки RMQ». Запись настроек в память носителя ПО СХСЗ производится по кнопке <Сохранить>.

При возврате к ресурсам самого СХСЗ следует использовать порт 5672 для брокера сообщений.

Для перехода на внешнюю БД необходимо задать в разделе «Настройки БД» IP-адрес, порт, имя базы данных, а также учетные данные для подключения – имя и пароль, после чего нажать кнопку <Сохранить>.

При вводе IP-адреса в настройках БД и RMQ проводится проверка на корректность его формата, и в случае указания неверного формата выдается соответствующее сообщение.

Для применения новых настроек работы БД и RMQ следует перезагрузить СХСЗ.

Также есть возможность перехода в режим отладки, необходимый для работ по диагностике Комплекса с участием производителя. По умолчанию данный режим отключен. Рекомендуется отключать его после выполнения всех необходимых работ, также этот режим отключается автоматически, если был выполнен выход Администратора из ПО сервисного режима работы СХСЗ.

3.5. Резервирование и восстановление СХСЗ

3.5.1. Общие сведения

В ПАК «Центр-Т» функция резервирования и восстановления настроек СХСЗ может быть реализована двумя способами:

- с использованием внешней БД (горячее резервирование);
- с использованием внутренней БД (холодное резервирование).

Резервирование с использованием внешней БД.

В этом случае используются два СХСЗ - основной и резервный. Оба подключаются к одной внешней БД (подробнее о настройке подключений к внешней БД – раздел 3.5.2). Каждый СХСЗ использует собственный внутренний брокер сообщений RMQ.

Не допускается подключение двух СХСЗ к общему брокеру сообщений.

Для клиентского устройства и утилиты удаленного управления СХСЗ в таком случае в настройках указываются два IP-адреса сервера RMQ.

Для клиентского устройства в настройках репозитория образов также должны быть указаны два IP-адреса - основного и резервного СХСЗ.

Схема подключения СХСЗ представлена на рисунке 15.

При таком резервировании в случае выхода из строя основного СХСЗ подключение клиентских устройств к резервному СХСЗ произойдет автоматически, а подключение утилиты удаленного управления - при нажатии кнопки «Проверить подключение».

В случае использования указанной схемы резервирования рекомендуется периодическое создание бекапов внешней БД.

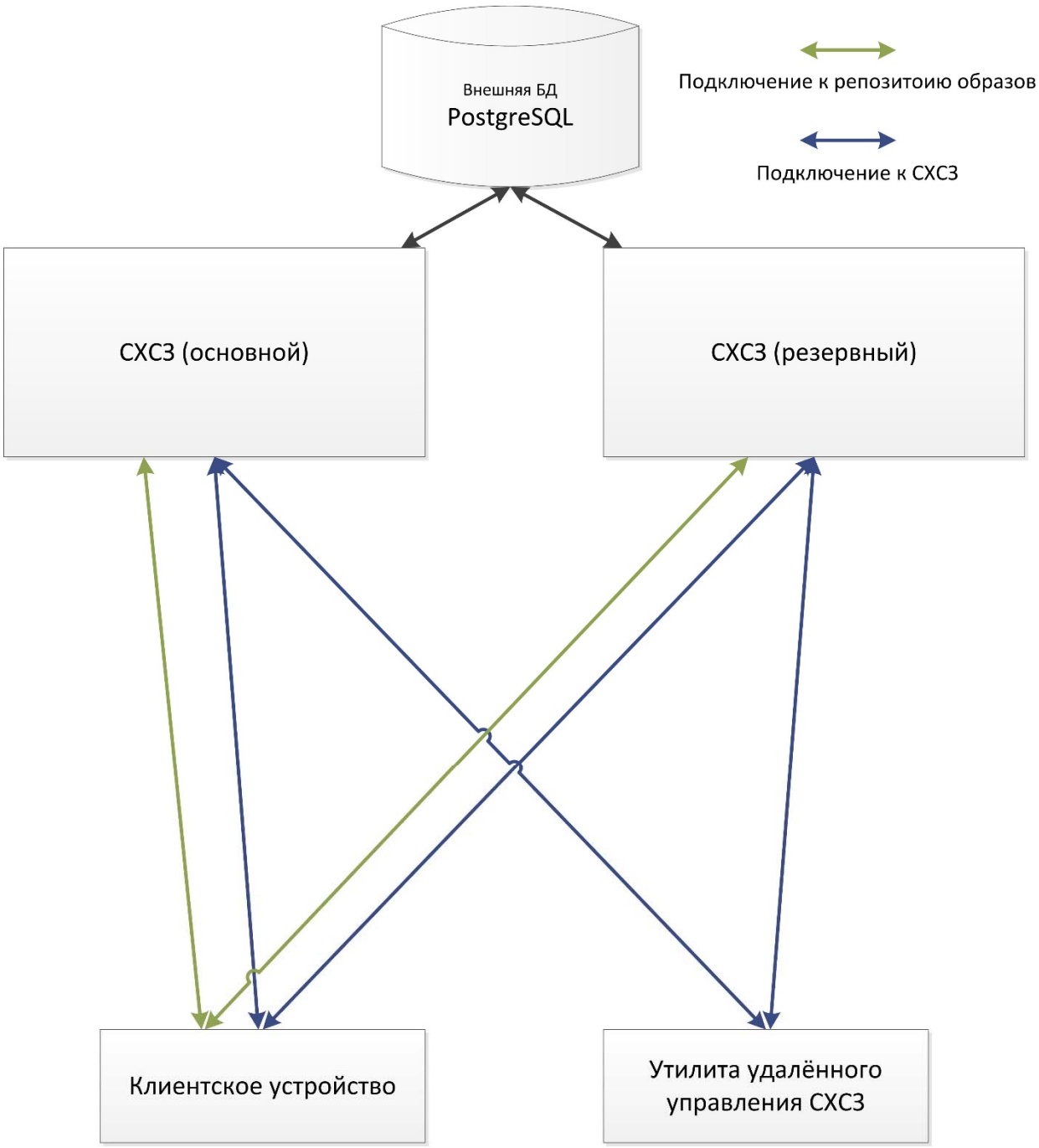


Рисунок 15 - Схема подключения СХСЗ при резервировании с использованием внешней БД

Резервирование с использованием внутренней БД

При такой схеме резервирования в один момент времени используется только один СХСЗ (основной). Резервный СХСЗ должен быть либо выключен, либо отключен от сети. На основном СХСЗ периодически выполняется резервирование настроек СХСЗ (резервирование внутренней БД). В случае выхода из строя основного СХСЗ следует восстановить из резервной копии БД на резервном СХСЗ и подключить его к сети. При этом сетевые настройки резервного СХСЗ должны быть заданы либо такие же, как на основном, и в этом случае на клиентских устройствах и в утилите удаленного управления задаются IP-адреса только основного сервера,

либо могут быть уникальными, а на клиентских устройствах и в утилите удаленного управления задаются IP-адреса и основного сервера, и резервного.

Периодичность, с которой Администратор сервисного режима должен выполнять резервирование базы данных СХСЗ, определяется в зависимости от частоты изменения настроек. Рекомендуется выполнять резервирование не реже чем раз в неделю.

3.5.2. Подключение внешнего носителя

Для получения возможности использования функции резервирования и восстановления БД СХСЗ необходимо смонтировать внешний носитель для экспорта/импорта настроек.

Монтирование внешнего носителя осуществляется на вкладке «USB Носитель» (рисунок 16).

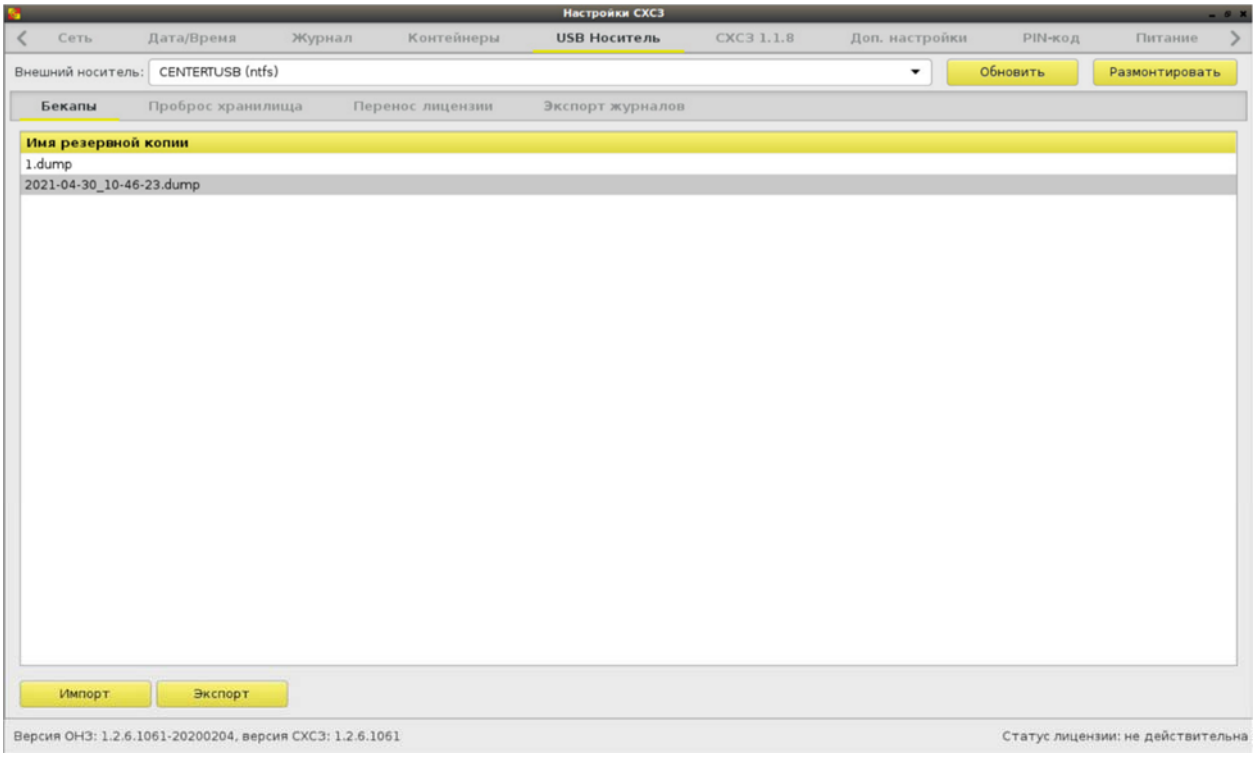


Рисунок 16 – Вкладка «USB Носитель»

После подключения внешнего носителя к разъему СХСЗ следует нажать кнопку <Обновить> (F5), выбрать его имя в строке «Внешний носитель», выбрать пункт «Бекапы» и нажать кнопку <Монтировать>.

После монтирования внешнего носителя на нем создается каталог «backups». Если такой каталог уже существует, в поле «Имя резервной копии» отображается его содержимое.

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).

Если загрузка СХСЗ выполнена на сервере HP, внешний носитель может быть проброшен через механизм iLO Remote Console. Для этого носитель следует подключить к ПЭВМ, на которой запущена iLO Remote Console, в меню отметить пункт «Virtual Drives» и выбрать носитель в списке (рисунок 17).

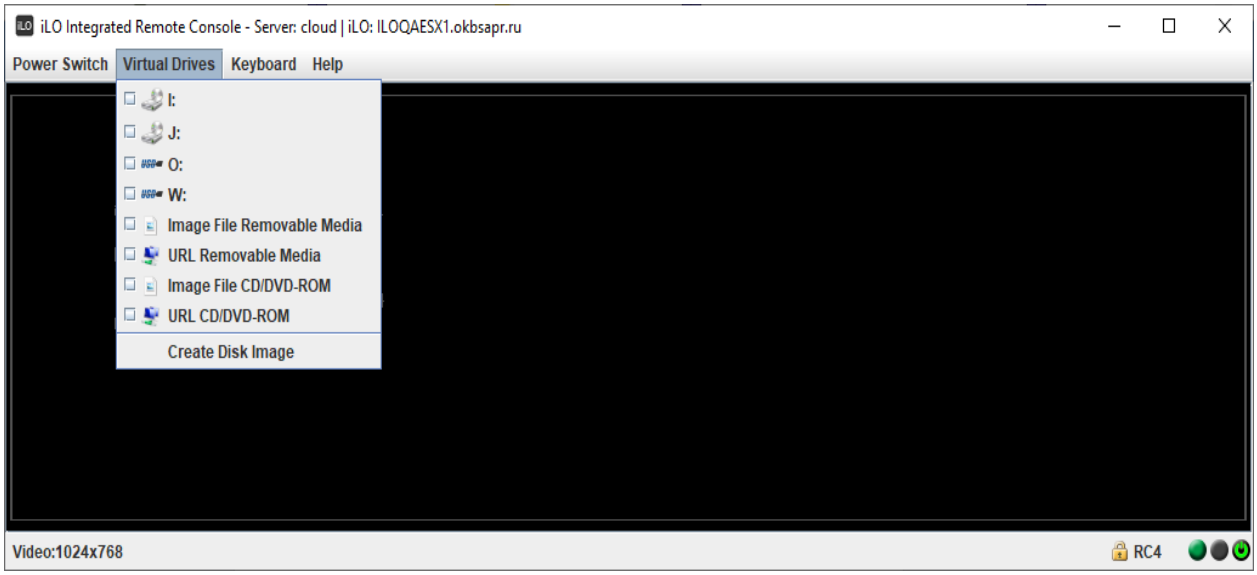


Рисунок 17 - Проброс внешнего носителя через iLO Remote Console

После этого носитель доступен к монтированию на вкладке «USB Носитель» (рисунок 16).

3.5.3. Резервирование внутренней БД СХСЗ

Резервирование внутренней базы данных СХСЗ выполняется на вкладке «USB Носитель» (рисунок 16) после подключения и монтирования носителя, на который должна быть экспортирована резервная копия настроек СХСЗ.

Для резервирования внутренней базы данных СХСЗ следует нажать кнопку <Экспорт>. При этом выполняется сохранение настроек СХСЗ на внешнем носителе, название файла с настройками отображается в поле «Имя резервной копии».

Файл с резервной копией настроек СХСЗ имеет расширение .dump.

Об успешном завершении процедуры свидетельствует соответствующее оповещение. При этом файл резервной копии отображается в поле «Имя резервной копии» (имя файла формируется, исходя из текущих даты и времени), а в журнале регистрации событий контейнера БД (CenterT-db) регистрируется остановка контейнера и последующий автоматический старт.

3.5.4. Восстановление внутренней БД СХСЗ

Восстановление внутренней базы данных СХСЗ выполняется после подключения и монтирования носителя с резервной копией настроек СХСЗ на вкладке «USB Носитель» (рисунок 16). Если на внешнем носителе в

каталоге «backups» содержится резервная копия настроек СХСЗ, она отображается в поле «Имя резервной копии».

Для восстановления внутренней базы данных СХСЗ следует нажать кнопку <Импорт>. Об успешном завершении процедуры свидетельствует соответствующее оповещение. При этом сохраняются настройки СХСЗ, содержащиеся в файле резервной копии, а в журнале регистрации событий контейнера БД (CenterT-db) регистрируются остановка контейнера и последующий автоматический старт.

Обратите внимание, что начиная с версии 1.2.5 были обновлены образы ПО ТС (см. перечень в разделе 5.5). При восстановлении БД из резервной копии, созданной на СХСЗ версии 1.2.4 и ниже, будет выполнено автоматическое преобразование имен образов ПО ТС, назначенных пользователям клиентского устройства.

Например, если пользователю в Центр-Т версии 1.2.4 был назначен образ citrix_13_8-vc-sso_nousb, то после восстановления резервной копии БД с такой настройкой на СХСЗ версии 1.2.5 и выше этому пользователю будет назначен citrix_13_10-vc-sso_nousb.

3.6. Настройка даты и времени

Настройка даты и времени на СХСЗ осуществляется на вкладке «Дата/Время» ПО сервисного режима работы (рисунок 18).

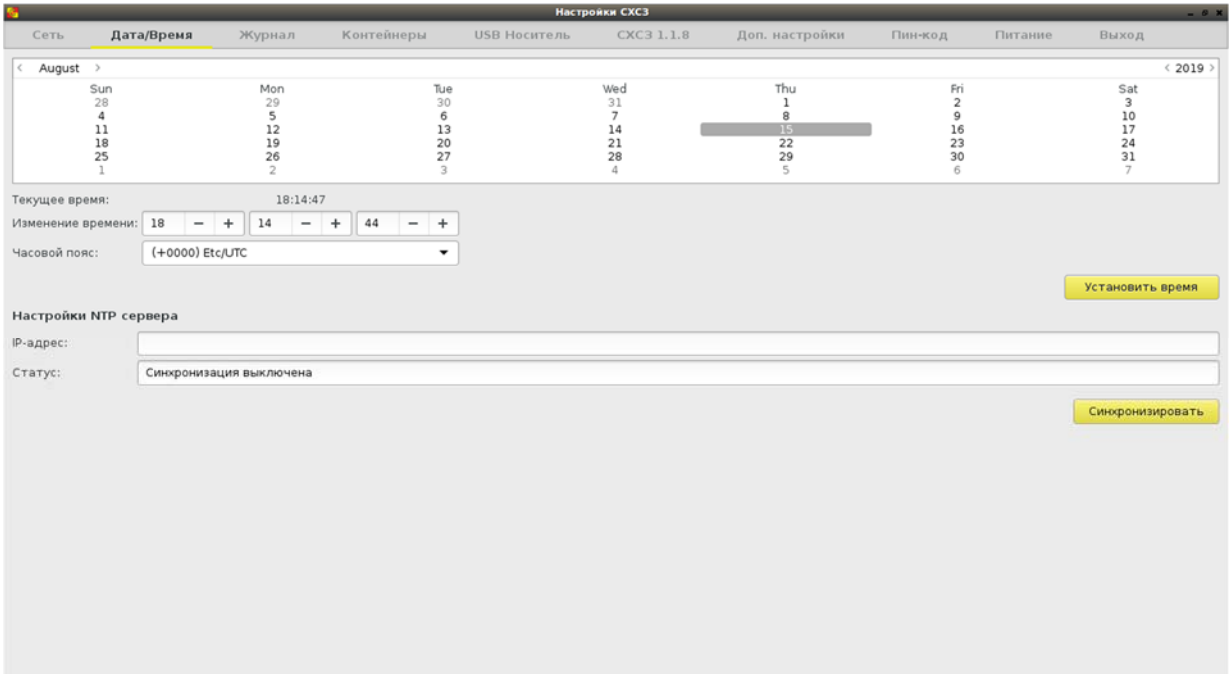


Рисунок 18 – Окно настройки даты и времени

Есть возможность изменить число, месяц и год, а также текущее время и часовой пояс. Сохранение параметров выполняется 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 19).

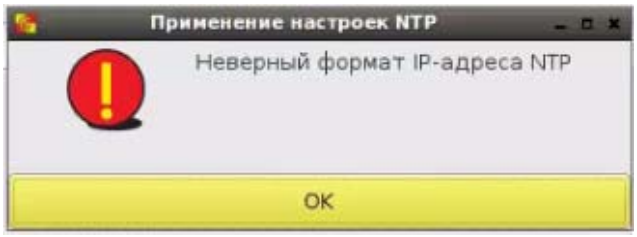


Рисунок 19 – Сообщение при вводе неверного формата IP-адреса

Особенности настройки даты и времени на СХСЗ на базе микрокомпьютера

При настройке времени на СХСЗ на базе защищенного микрокомпьютера следует учитывать, что после выключения или перезагрузки устройства на нем не сохраняются настройки даты и времени. Рекомендуется использовать внешний NTP-сервер.

Также следует учесть, что поле «Текущее время» отображает время перехода на вкладку «Дата/Время» и не обновляется автоматически. Обновление происходит при нажатии на кнопку .

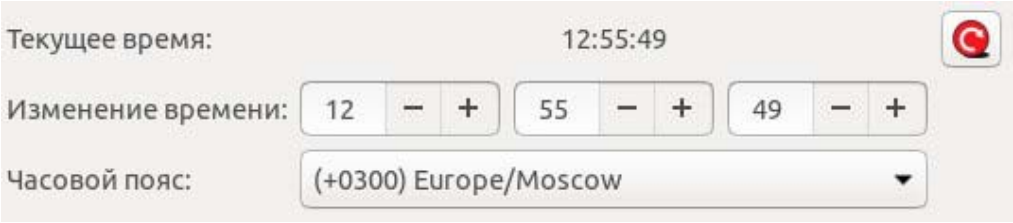


Рисунок 20 – Настройка времени на СХСЗ на базе защищенного микрокомпьютера

3.7. Мониторинг состояния контейнеров

В ПАК «Центр-Т» используется технология контейнеризации. Каждый контейнер содержит данные определенного назначения:

- ПО Комплекса (контейнер CenterT-app);
- БД (контейнер CenterT-db);
- брокер сообщений (контейнер CenterT-broker);
- хранилище с образами ПО ТС (контейнер CenterT-store).

Чтобы просмотреть статус контейнера, следует перейти на вкладку «Контейнеры» (рисунок 21). Обновление информации будет происходить статично, если вкладка остается открытой.

Контейнеры настроены таким образом, что в случае сбоя ПО производится их автоматический перезапуск.

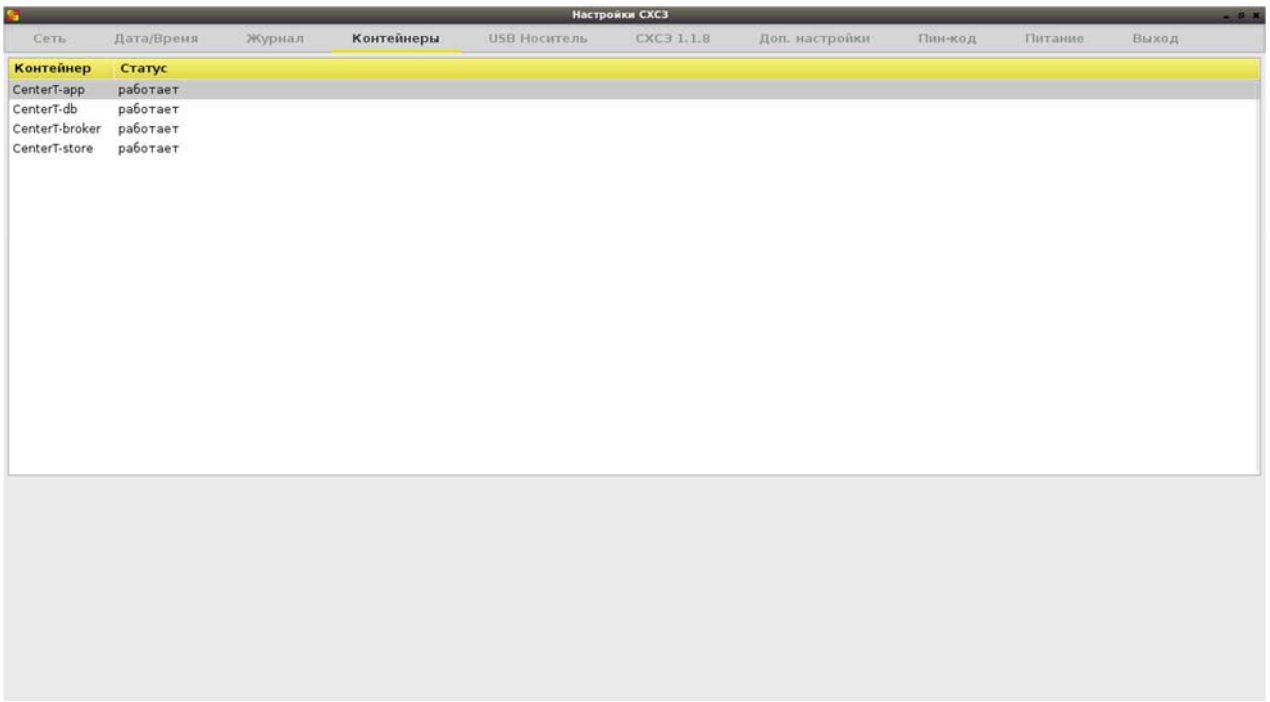


Рисунок 21 – Вкладка «Контейнеры»

3.8. Смена PIN-кода Администратора сервисного режима

Для смены PIN-кода предназначена вкладка «PIN-код» (рисунок 1).

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).

3.9. Просмотр событий безопасности

Администратор сервисного режима может просмотреть события безопасности:

- собственной сессии;
- контейнеров СХСЗ.

Для этого служит вкладка «Журнал» (рисунок 22).

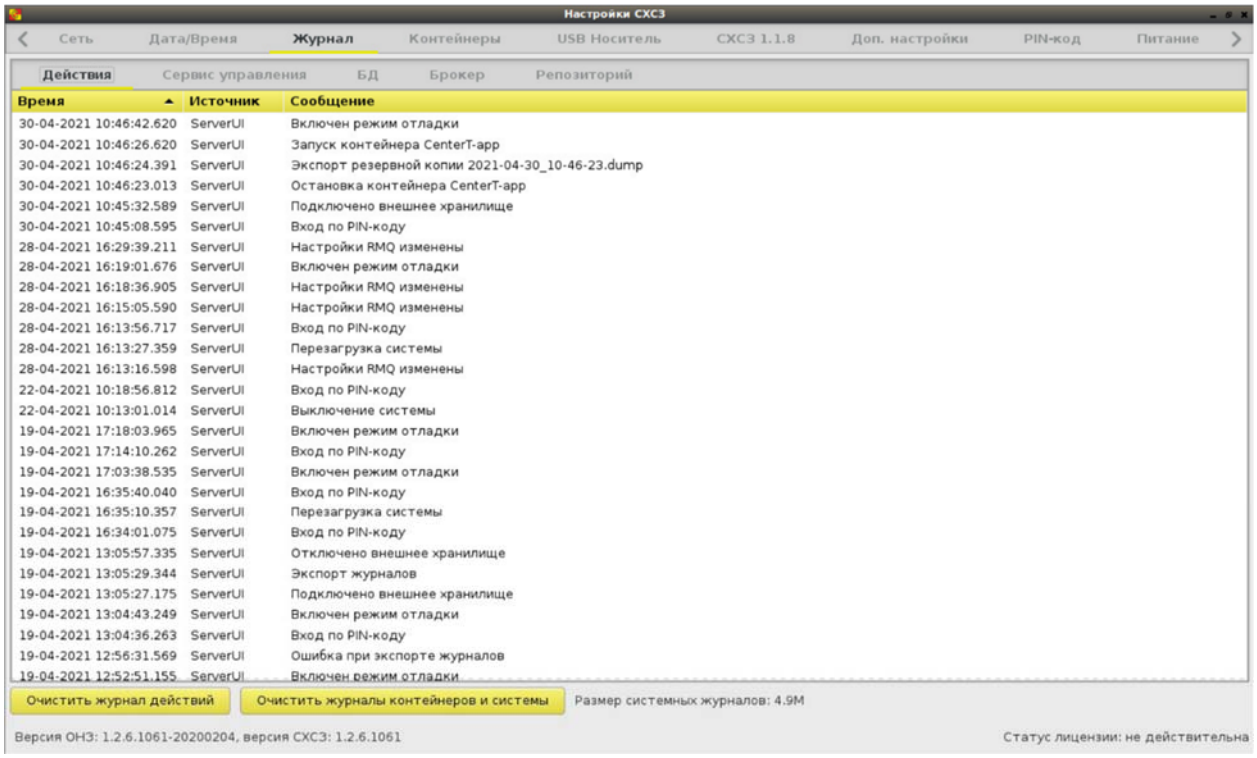


Рисунок 22 – Вкладка «Журнал»

События безопасности собственной сессии отображаются на вкладке «Действия» в окне просмотра журналов.

События безопасности контейнеров СХСЗ распределены по вкладкам:

- «Сервис управления» – контейнер с ПО СХСЗ;
- «БД» – контейнер с БД;
- «Брокер» – контейнер брокера сообщений;
- «Репозиторий» – контейнер с образами ПО ТС.

Для каждого события регистрируются:

- время;
- источник/контейнер;
- сообщение.

ВНИМАНИЕ! Время событий для вкладки «Действия» указывается UTC, а для всех остальных вкладок («Сервис управления», «БД», «Брокер», «Репозиторий») – текущее время.

Журналы событий безопасности собственной сессии сохраняются в локальной базе данных и не перезаписываются при выключении/перезагрузке сервера.

Журналы событий безопасности контейнеров СХСЗ перезаписываются при каждом выключении/перезагрузке сервера.

При условии долгой непрерывной работы сервера максимальный размер, который могут занять журналы событий безопасности контейнеров СХСЗ, составляет 19,9МБ. При достижении этого значения файлы с сообщениями о событиях безопасности будут циклически перезаписываться.

Журналы регистрации действий и журналы контейнеров и системы можно принудительно очистить. Для очистки журнала событий безопасности собственной сессии следует нажать кнопку <Очистить журнал действий> (рисунок 22). Появится предложение о предварительном экспорте данных журнала на внешний носитель (рисунок 23).

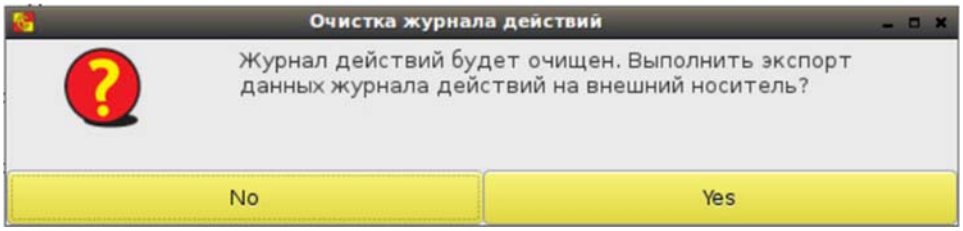


Рисунок 23 – Предложение о предварительном экспорте журнала перед очисткой

При согласии на экспорт журнала следует иметь в виду, что внешний носитель, на который планируется осуществить экспорт, должен быть примонтирован к СХСЗ (подробнее об этом - п.3.10), иначе появится соответствующее сообщение об ошибке. Об успешном копировании данных журнала действий также появится сообщение (рисунок 24).

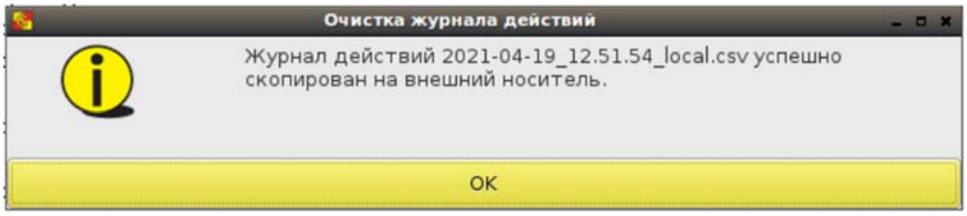


Рисунок 24 – Сообщение об успешном экспорте данных журнала действий на внешний носитель

Если предварительный экспорт журнала не требуется, то при нажатии кнопки <No> (или при нажатии <OK> на рисунке 24) появится вопрос о непосредственной очистке журнала действий (рисунок 25).

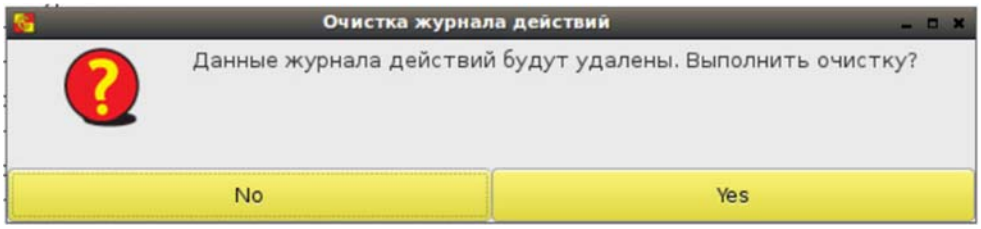


Рисунок 25 – Окно очистки данных журнала действий

При успешной очистке журнала действий появляется соответствующее сообщение (рисунок 26).

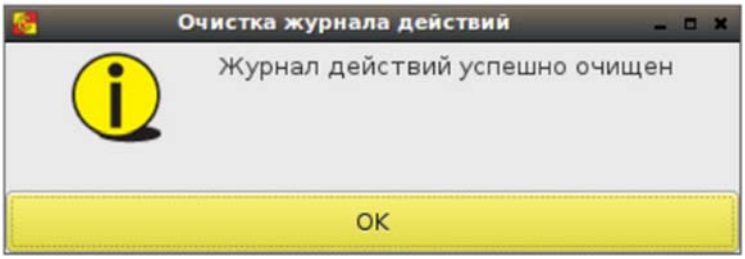


Рисунок 26 – Сообщение об успешной очистке журнала действий

При необходимости очистки журналов контейнеров и системы следует нажать кнопку <Очистить журналы контейнеров и системы> (рисунок 22). Алгоритм очистки аналогичен описанному выше.

Системные журналы недоступны к просмотру, можно только просмотреть их размер (справа от кнопок очистки журналов).

3.10. Экспорт журналов событий безопасности

Экспорт журналов событий безопасности доступен на вкладке "USB Носитель" –> "Экспорт журналов" (рисунок 27).

Внешний носитель, на который планируется осуществить экспорт, следует подключить к разъему СХСЗ, далее нажать кнопку <Обновить> (F5), выбрать его имя в строке «Внешний носитель» и нажать кнопку <Монтировать>. После успешного монтирования следует в поле «Выбор журналов для экспорта» отметить необходимые журналы и нажать кнопку <Экспорт>.

Файлы журналов будут созданы в директории logs внешнего носителя (при необходимости создается автоматически).

При успешном экспорте журналов на внешний носитель появится соответствующее сообщение с указанием имен созданных файлов (рисунок 28).

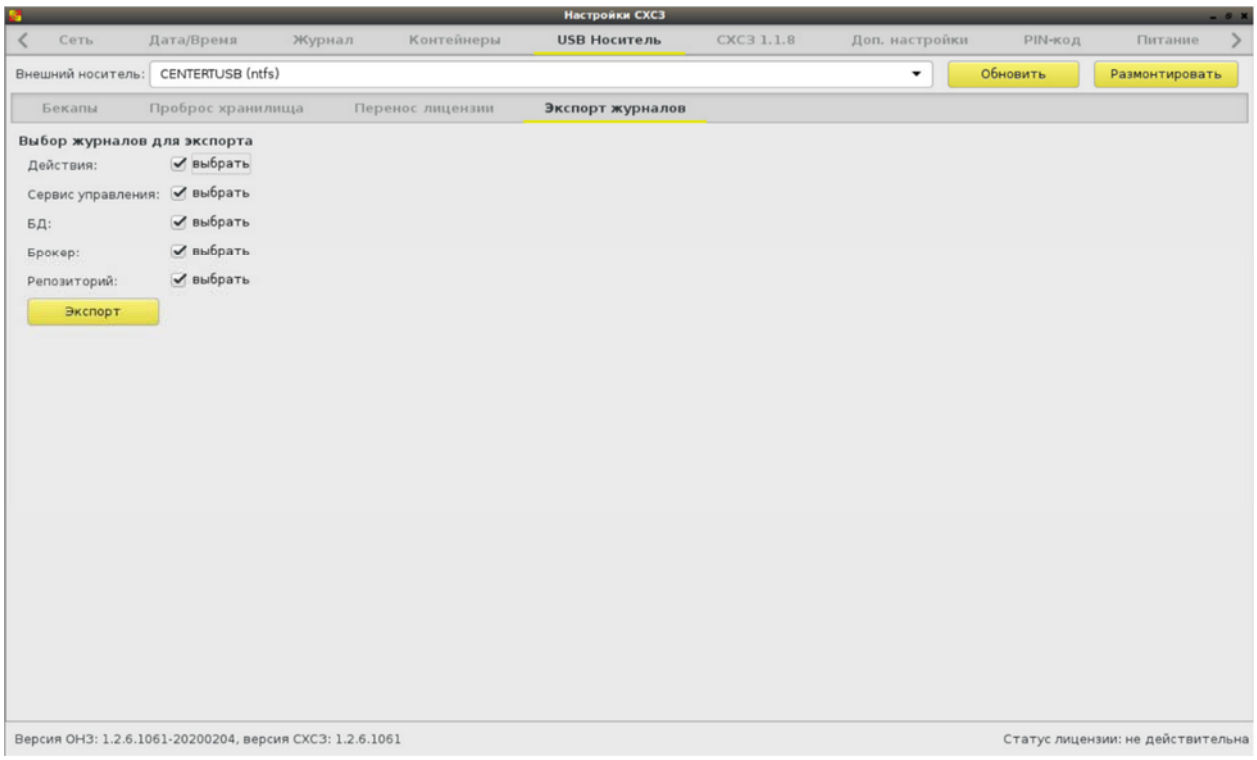


Рисунок 27 – Вкладка "USB Носитель" –> "Экспорт журналов"

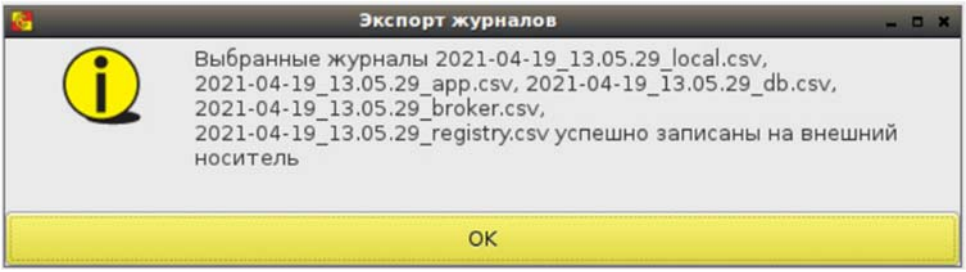


Рисунок 28 – Сообщение об успешном экспорте журналов на внешний носитель

3.11. Завершение работы СХСЗ

Для завершения работы Администратор сервисного режима может:

- завершить работу ПО сервисного режима;
- заблокировать сессию.

Для завершения работы СХСЗ можно нажать кнопку питания на СВТ[4] или перейти на вкладку «Питание» (рисунок 29) и выбрать действие (выключить или перезагрузить) кнопкой <выполнить>.

В случае использования СХСЗ на базе защищенного микрокомпьютера для завершения работы дополнительно следует нажать кнопку на шнуре питания.

---

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

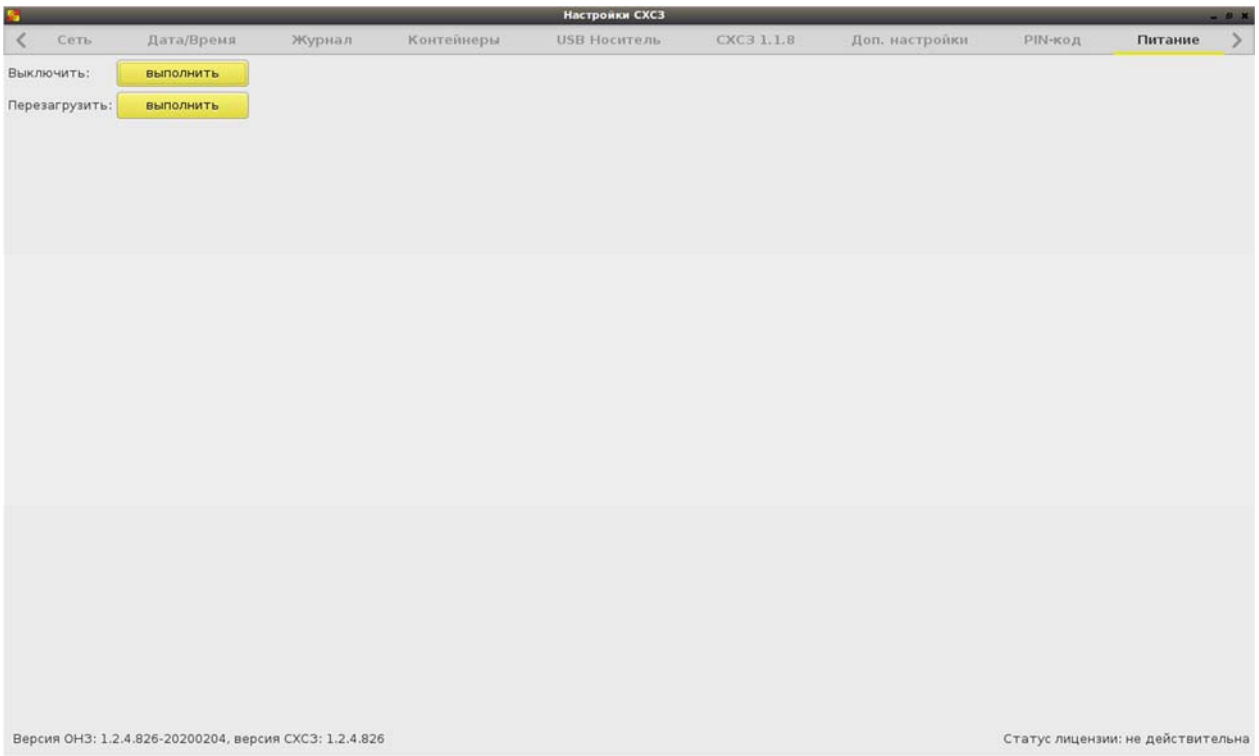


Рисунок 29 – Вкладка «Питание»

Для блокирования сессии работы ПО сервисного режима необходимо перейти на вкладку «Выход». При этом появляется окно блокировки, изображенное на рисунке 30.

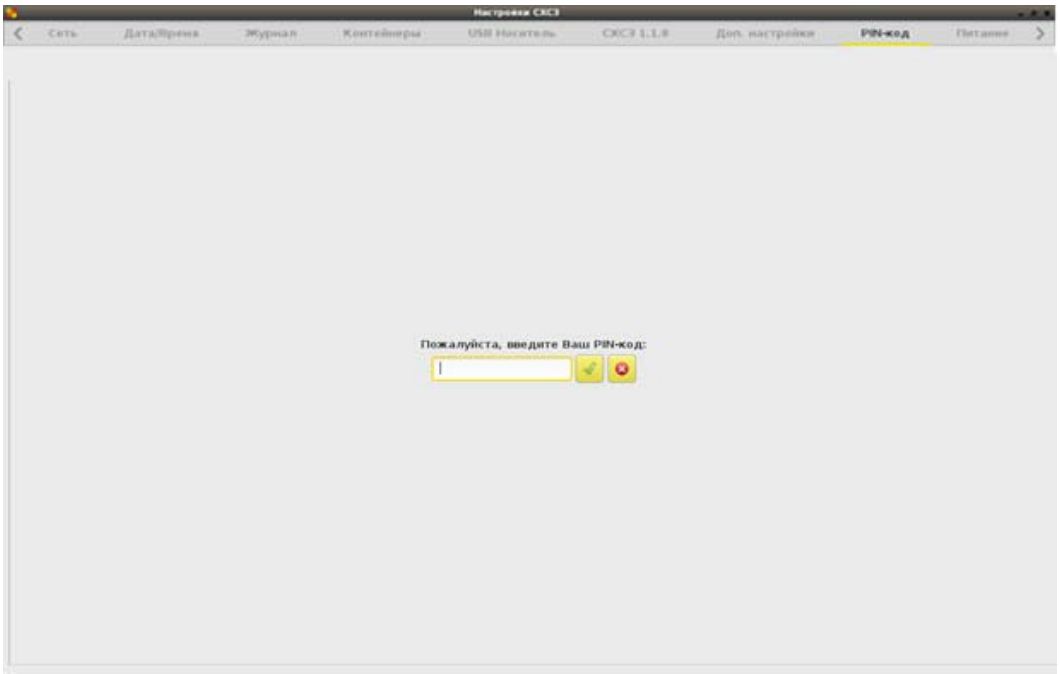


Рисунок 30 – Экран блокировки ПО сервисного режима

Для выхода из режима блокировки следует ввести верный PIN-код и нажать кнопку (<Enter>).

4. Состав работ Администратора

4.1. Общие сведения

Администратор СХСЗ приступает к выполнению своих функциональных обязанностей после того как Администратор сервисного режима запустил СХСЗ и выполнил установку сетевых настроек. В рамках своих обязанностей Администратор СХСЗ осуществляет следующие действия:

1) устанавливает ПО для удаленного доступа к СХСЗ на АРМ Администратора (см. 4.2);

2) получает доступ к ПО управления СХСЗ (см. 4.3);

3) если планируется использование созданных по умолчанию учетных записей Администратора и Администратора БИ – назначает собственный идентификатор и меняет пароль Администратора (см. 4.4). Если планируется использование учетных записей администраторов удаленного управления СХСЗ, созданных при настройке Комплекса:

– создает на СХСЗ две новые учетные записи для Администратора и Администратора безопасности информации (по умолчанию все создаваемые учетные записи имеют роль «Пользователь клиентского устройства») (см. 4.5.1);

– обращается к Администратору БИ для назначения новым учетным записям административных ролей;

– использует новую собственную учетную запись, при первом входе меняет для нее пароль и назначает идентификатор (см. 4.4);

4) управляет учетными записями пользователей (см. 4.5);

5) задает параметры терминала пользователя (см. 4.6);

6) просматривает информацию об используемом Клиентами оборудовании (см 4.7);

7) управляет шаблонами настроек образов ПО ТС (см. 4.8).

При эксплуатации Комплекса Администратор СХСЗ по мере необходимости может менять собственные параметры идентификации (см. 4.4) и просматривать события безопасности собственной сессии (см. 4.9).

4.2. Установка ПО для удаленного доступа к СХСЗ

Для установки ПО, требуемого для получения удаленного доступа к ПО управления СХСЗ, необходимо запустить **от имени администратора** исполняемый файл на диске «Центр-Т». При запуске файла появляется окно мастера установки ПО (рисунок 31).

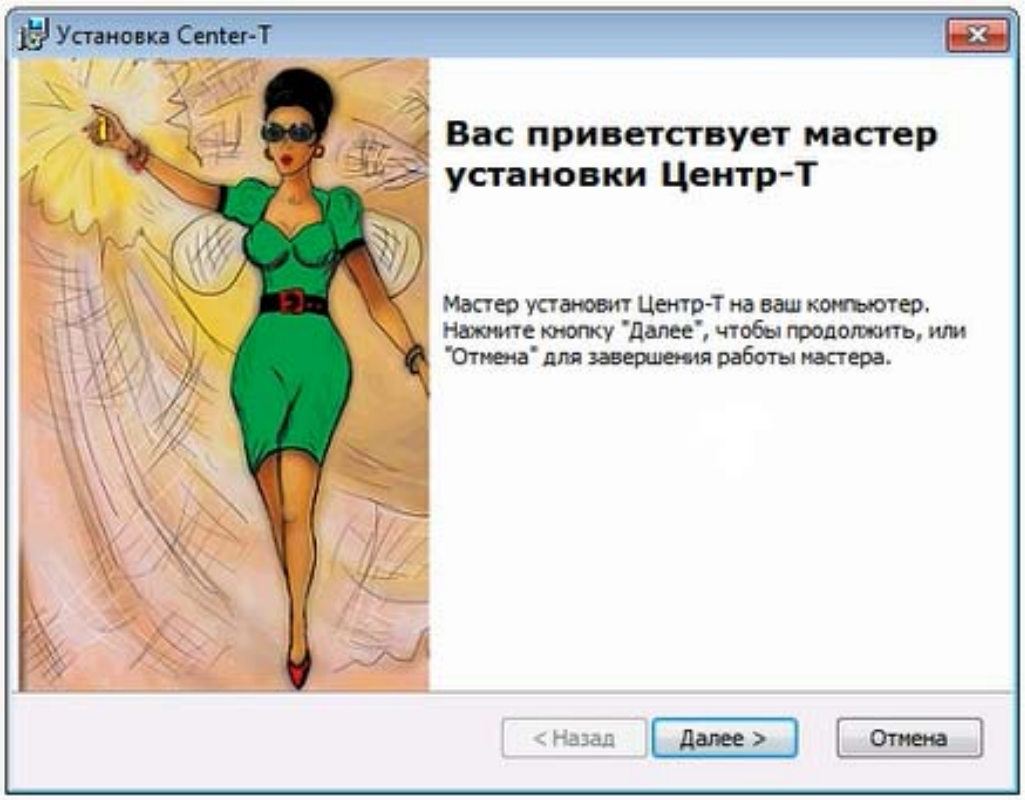


Рисунок 31 – Окно мастера установки ПО удаленного доступа

При нажатии кнопки <Далее> появляется окно выбора каталога для установки ПО (рисунок 32).

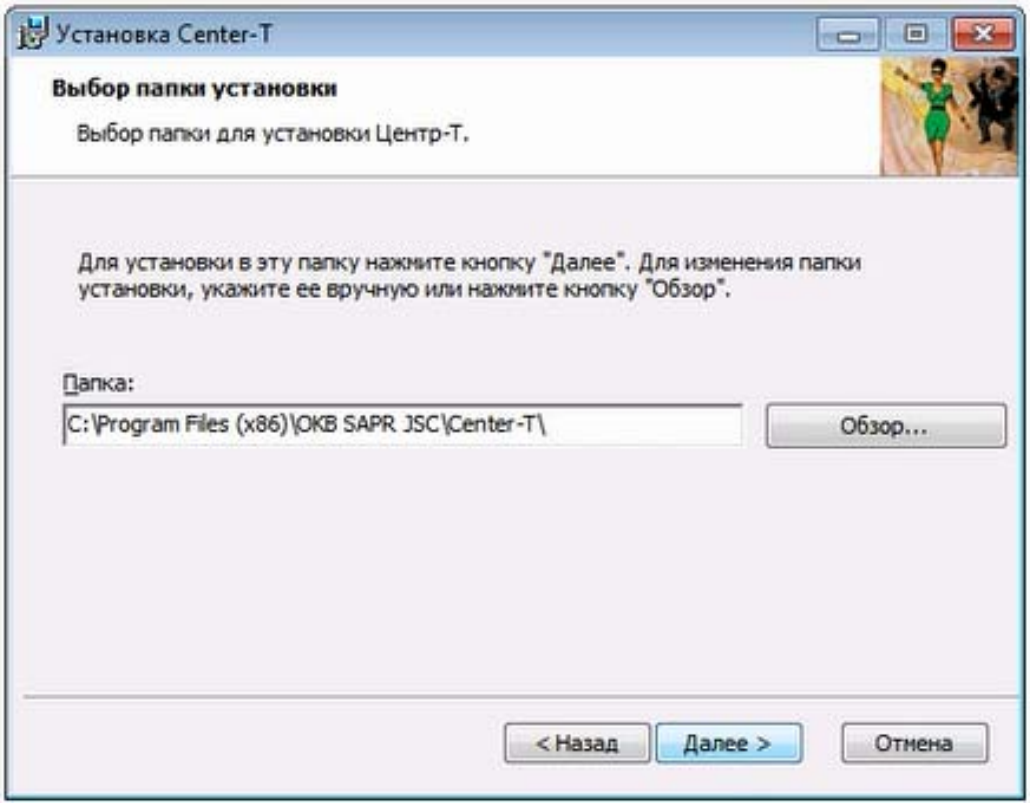


Рисунок 32 – Окно выбора каталога для установки ПО

Если необходимо изменить предлагаемый каталог для установки, следует нажать кнопку <Обзор…> и указать новое расположение ПО.

По кнопке <Далее> появляется окно для указания сетевых параметров сервера RabbitMQ, используемого СХСЗ (рисунок 33). В случае резервирования СХСЗ необходимо указать IP-адреса сервера RabbitMQ и для основного, и для резервного СХСЗ.

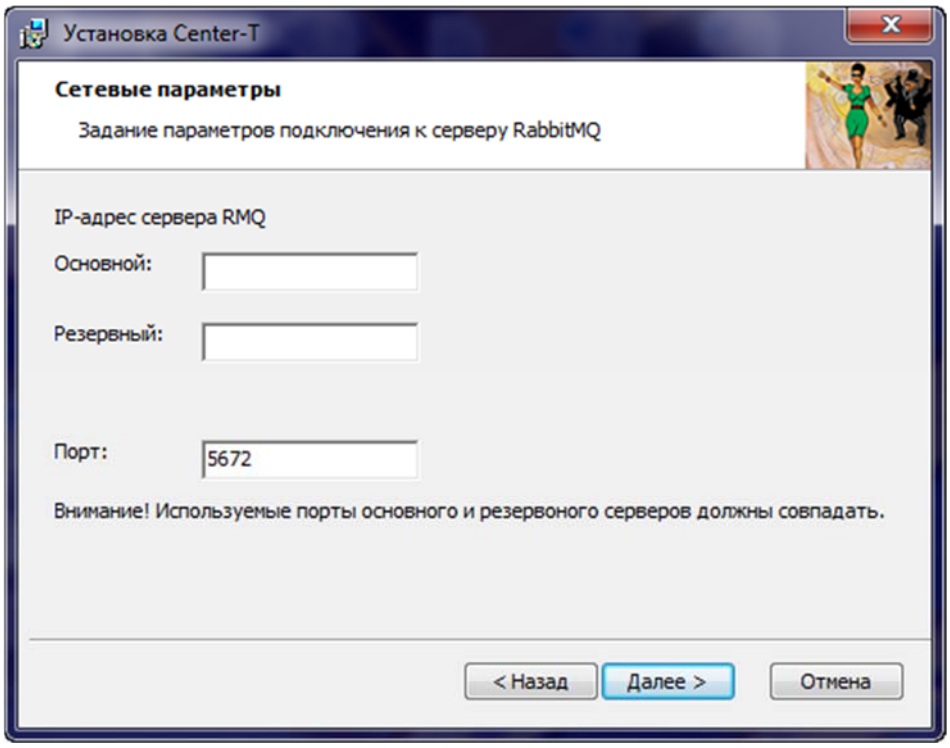


Рисунок 33 – Окно для указания сетевых параметров СХСЗ

Адреса и порт можно получить у Администратора сервисного режима. Если в качестве брокера сообщений используется брокер из контейнера на СХСЗ, то порт по умолчанию для сервера RabbitMQ – 5672. После указания запрашиваемых данных следует нажать <Далее> и следовать подсказкам мастера установки.

В результате успешной установки ПО появляется окно с сообщением о завершении работы мастера и возможности работы с установленным ПО.

4.3. Получение доступа к ПО управления СХСЗ

Для получения доступа к ПО управления СХСЗ следует запустить приложение для удаленного доступа к СХСЗ. При этом появляется окно идентификации, изображенное на рисунке 34.

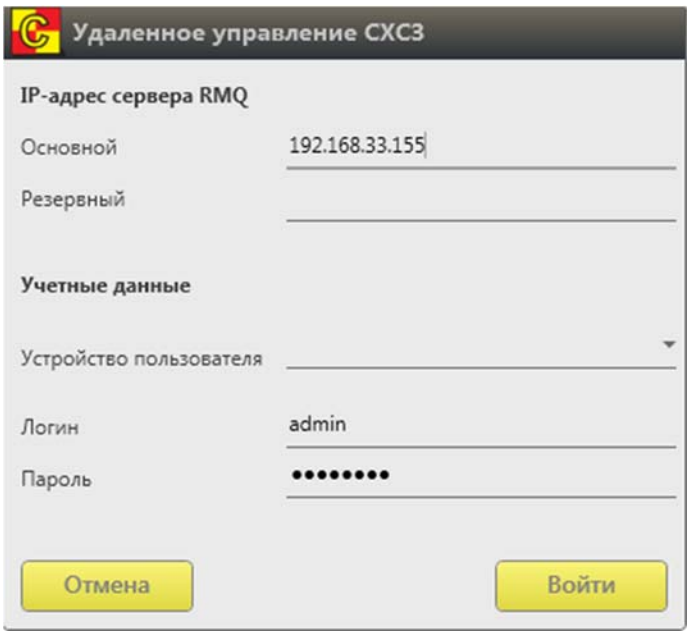


Рисунок 34 – Окно идентификации при первом доступе к ПО управления

Если в качестве брокера сообщений используется брокер из контейнера на текущем СХСЗ, в строке «IP-адрес сервера RMQ» указывается то значение параметра, которое установлено Администратором сервисного режима при настройке IP-адреса СХСЗ.

Администратору необходимо ввести логин, пароль, а также подключить к компьютеру свой идентификатор. В качестве идентификатора могут использоваться Специальные носители Центр-Т 4ГБ и 8ГБ, а также ШИПКА-лайт, ШИПКА-лайт slim. После заполнения всех строк следует нажать кнопку <Войти>.

ВНИМАНИЕ! Если в качестве идентификатора используется Специальный носитель Центр-Т 8ГБ, на АРМ Администратора должно быть установлено ПО Специального носителя ПО ПАК «Центр-Т» (подробнее об установке ПО см. Приложение 4).

При первом доступе к ПО управления СХСЗ Администратору необходимо использовать логин и пароль, установленные для него по умолчанию – логин admin и пароль P@ssw0rd; идентификатор при этом предъявлять не требуется (если идентификатор уже подключен и отображается в устройстве пользователя, то при первом входе его значение будет проигнорировано). После входа в ПО управления СХСЗ выполняется принудительное изменение пароля и назначение собственного идентификатора. Порядок выполнения процедуры назначения устройства и нового пароля указан в пункте 4.4.

В дальнейшем смена пароля/идентификатора может быть произведена в любое время.

Все последующие действия должны выполняться от имени той учетной записи, которую планируется использовать для работы с СХСЗ.

Если идентификация Администратора выполнена успешно, появляется главное окно ПО управления СХСЗ с доступными Администратору настройками (рисунок 35).

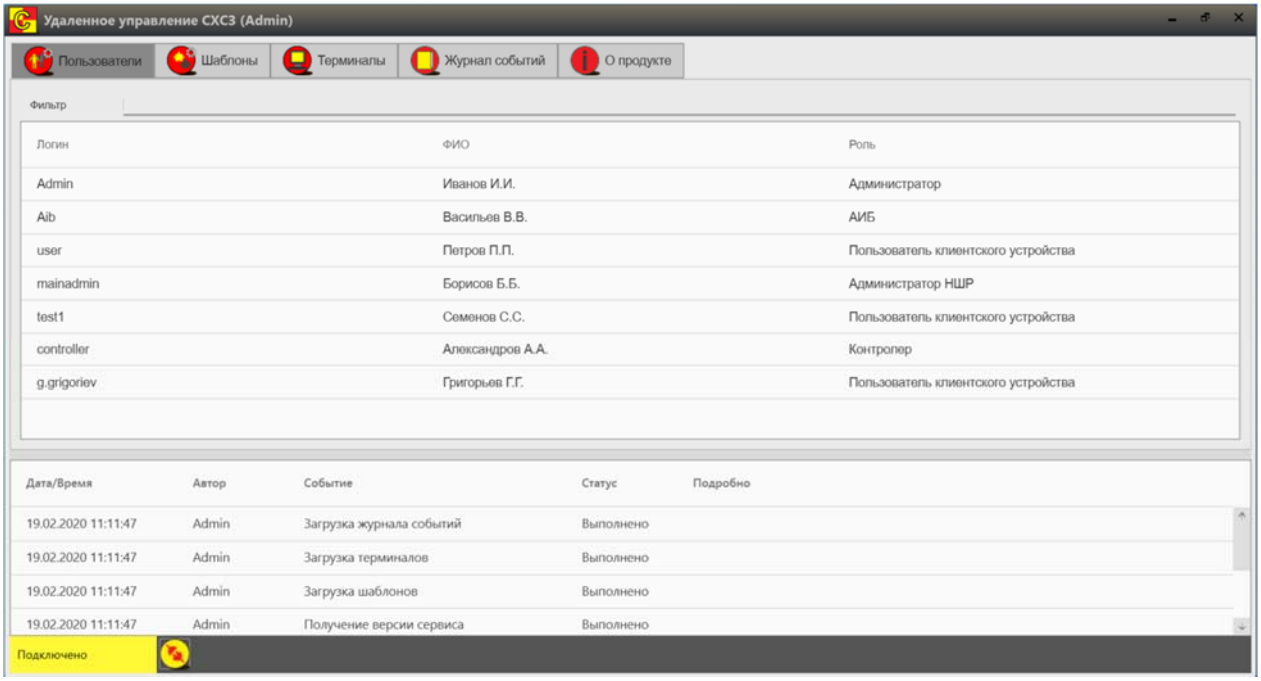


Рисунок 35 – Вкладка «Пользователи»

При первом запуске ПО управления в БД пользователей есть только две учетные записи, созданные по умолчанию, – Admin и Aib.

Учетная запись, от имени которой работает Администратор, указана в строке с названием утилиты.

4.4. Изменение параметров идентификации Администратора

Для идентификации Администратор использует пароль и отчуждаемое аппаратное устройство.

Для изменения параметров идентификации в процессе эксплуатации СХСЗ Администратору необходимо перейти на вкладку «Пользователи» в главном окне ПО управления СХСЗ и выбрать собственную учетную запись. Далее по щелчку правой кнопкой мыши следует вызвать окно доступных действий и выбрать пункт «Редактировать» или нажать на выделенной записи клавишу «Enter». При этом появляется окно настроек учетной записи Администратора (рисунок 36).

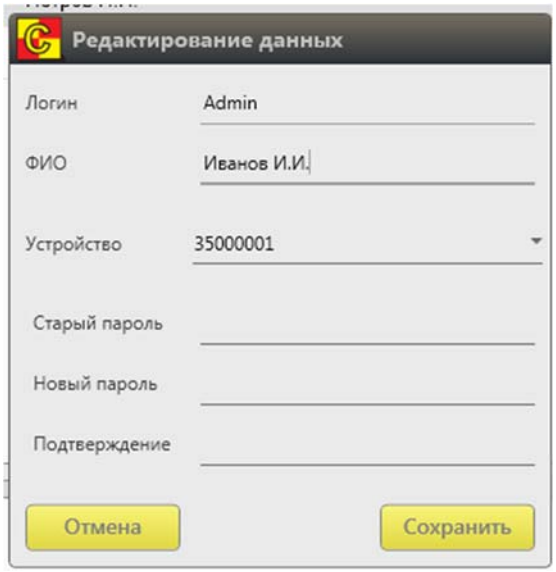


Рисунок 36 – Окно настроек учетной записи Администратора

В появившемся окне Администратор может изменить собственные логин, ФИО, а также назначить новый пароль и новый идентификатор. Чтобы назначить новый идентификатор, необходимо подключить устройство к ПК и выбрать его в списке поля «Устройство».

Сохранение параметров аутентификации Администратора выполняется по кнопке <Сохранить>. После выполнения необходимых настроек следует перезапустить утилиту.

4.5. Управление учетными записями

4.5.1. Создание учетных записей

Для создания новой учетной записи необходимо на вкладке «Пользователи» нажать правой кнопкой мыши в любом месте таблицы учетных записей и выбрать пункт «Создать» в меню доступных действий. При этом появляется окно создания учетной записи пользователя (рисунок 37).

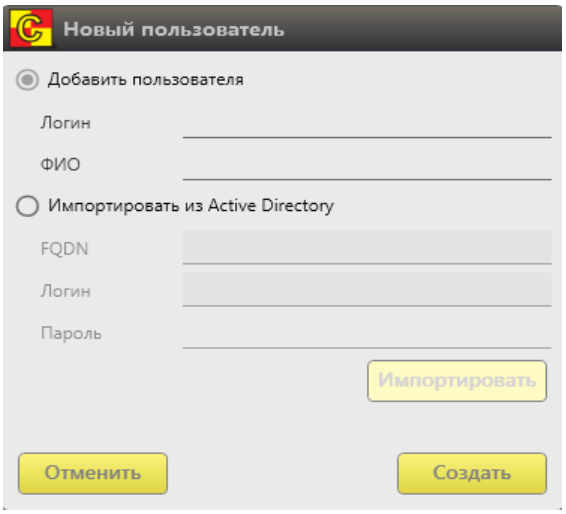


Рисунок 37 – Окно создания учетной записи

Учетную запись можно создать двумя способами:

–вручную;

–импортировать из Active Directory (AD).

Если нужно создать учетную запись вручную, следует установить флаг «Добавить пользователя» и указать логин и ФИО пользователя в соответствующих полях.

Для добавления учетной записи пользователя из AD нужно установить флаг «Импортировать из Active Directory» (рисунок 38) и указать FQDN сервера службы AD, а также логин пользователя и пароль, соответствующие учетной записи в AD пользователя, у которого есть права на чтение подраздела «Пользователи» (наличие специализированных прав доступа не обязательно).

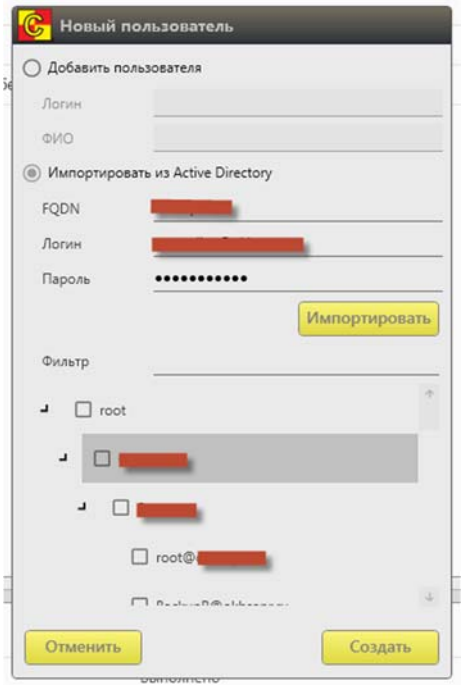


Рисунок 38 - Добавление учетной записи пользователя из AD

Для продолжения необходимо нажать кнопку <Импортировать>. При этом текущее окно расширяется, и в нижней части окна появляется структура подразделений AD, где можно выбрать для добавления как отдельных пользователей, так и целое подразделение. Для поиска конкретного подразделения в структуре AD можно воспользоваться фильтром: в поле «Фильтр» ввести имя или часть имени подразделения и нажать клавишу «Enter». В этом случае в поле структуры AD будут отображаться только подразделения, удовлетворяющие результатам поиска.

Применение изменений осуществляется по кнопке <Создать>. Все созданные учетные записи отображаются в таблице на вкладке «Пользователи».

ВНИМАНИЕ! Рекомендуется создавать резервные учетные записи для Администратора и Администратора БИ на случай, если пароль или идентификатор используемой учетной записи будет утерян.

Для каждого пользователя отображается следующая информация:

- логин;
- ФИО;
- роль.

Если зарегистрировано множество учетных записей пользователей, то весь перечень может не умещаться в отображаемом списке. Для поиска нужной учетной записи можно использовать функцию фильтра, доступную в верхней части окна (рисунок 35). Применение фильтра происходит по нажатию на клавишу «Enter», поиск осуществляется с учетом регистра. Для удаления фильтра необходимо удалить искомый текст и вновь нажать клавишу «Enter».

4.5.2. Редактирование учетных записей

Для изменения параметров учетной записи необходимо на вкладке «Пользователи» выбрать нужную запись и вызвать контекстное меню нажатием правой кнопки мыши. В появившемся окне следует выбрать пункт «Редактировать». При этом на экране появляется окно редактирования учетной записи пользователя (рисунок 39).

В случае редактирования учетных записей администраторов удаленного управления СХСЗ Администратору СХСЗ доступна смена ФИО и логина.

В случае редактирования учетных записей пользователей клиентского устройства Администратору СХСЗ доступны:

- смена ФИО и логина;
- настройка разрешения экрана (возможно после осуществления первого подключения Пользователя к СХСЗ);
- настройка параметров кэширования образа ПО ТС на устройстве пользователя;
- просмотр следующих параметров: дата и время последнего подключения, объем свободной памяти момент старта ОНЗ, настройки сети (IP-адрес терминала, загруженного с клиентского устройства пользователя), интервал подключения к сервису RMQ (рисунок 40).

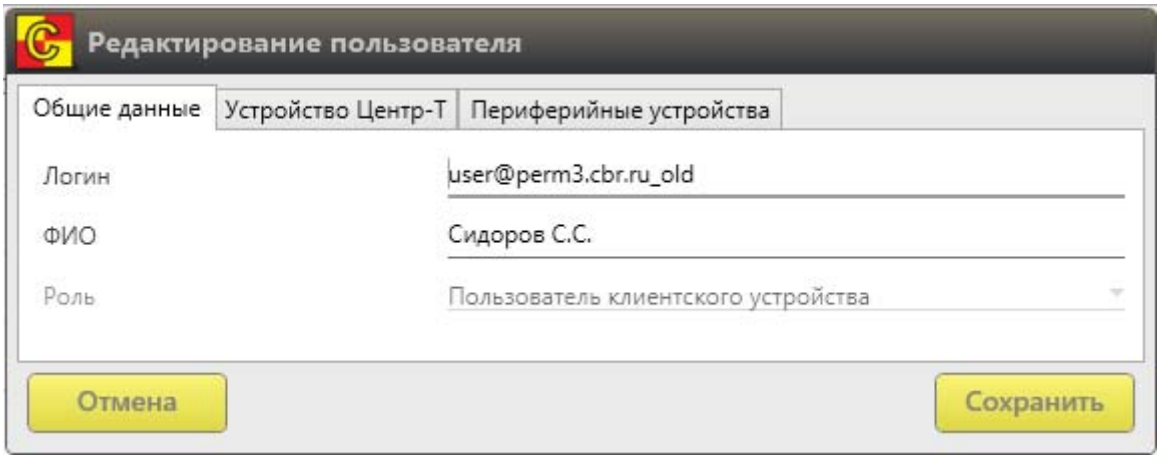


Рисунок 39 - Окно редактирования учетной записи пользователя. Общие данные

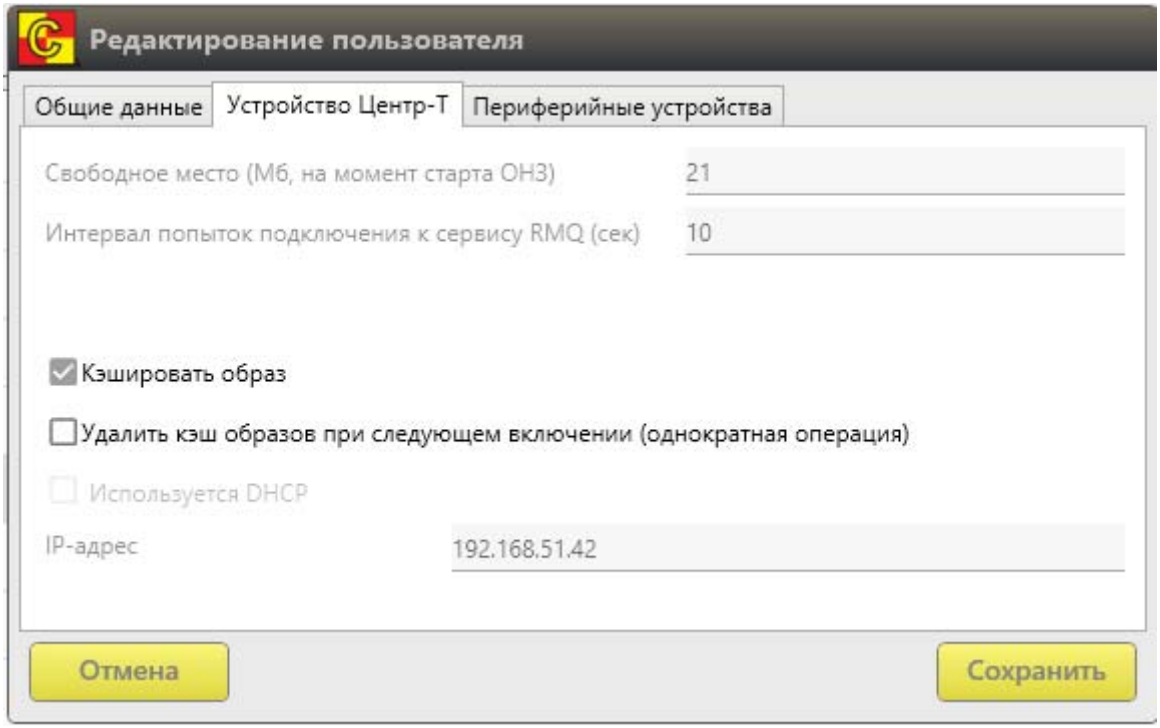


Рисунок 40 - Окно редактирования учетной записи пользователя. Устройство Центр-Т

При редактировании собственной учетной записи Администратору СХСЗ помимо смены логина и ФИО доступны также изменения пароля и идентификатора (рисунок 41).

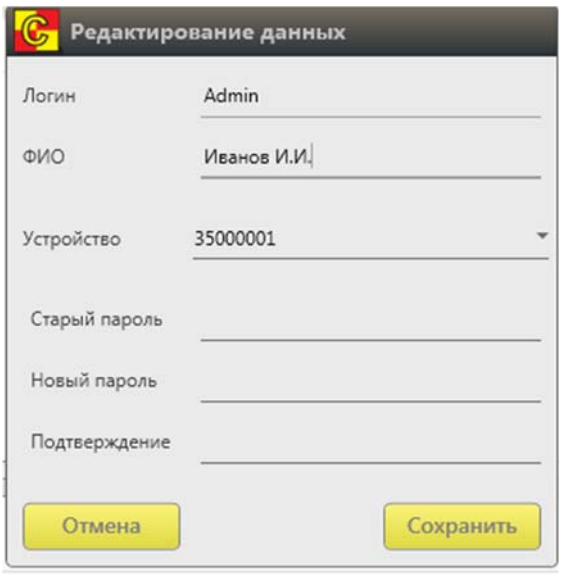


Рисунок 41 - Окно редактирования учетной записи Администратора СХСЗ

4.5.2.1. Настройка разрешения экрана

Администратор СХСЗ может удаленно изменить разрешение экрана пользователя. Для этого на вкладке «Периферийные устройства» в окне редактирования пользователя нужно указать одно из доступных разрешений экрана (рисунок 42). Если рабочее место пользователя предусматривает несколько мониторов, то предварительно нужно выбрать нужный монитор.

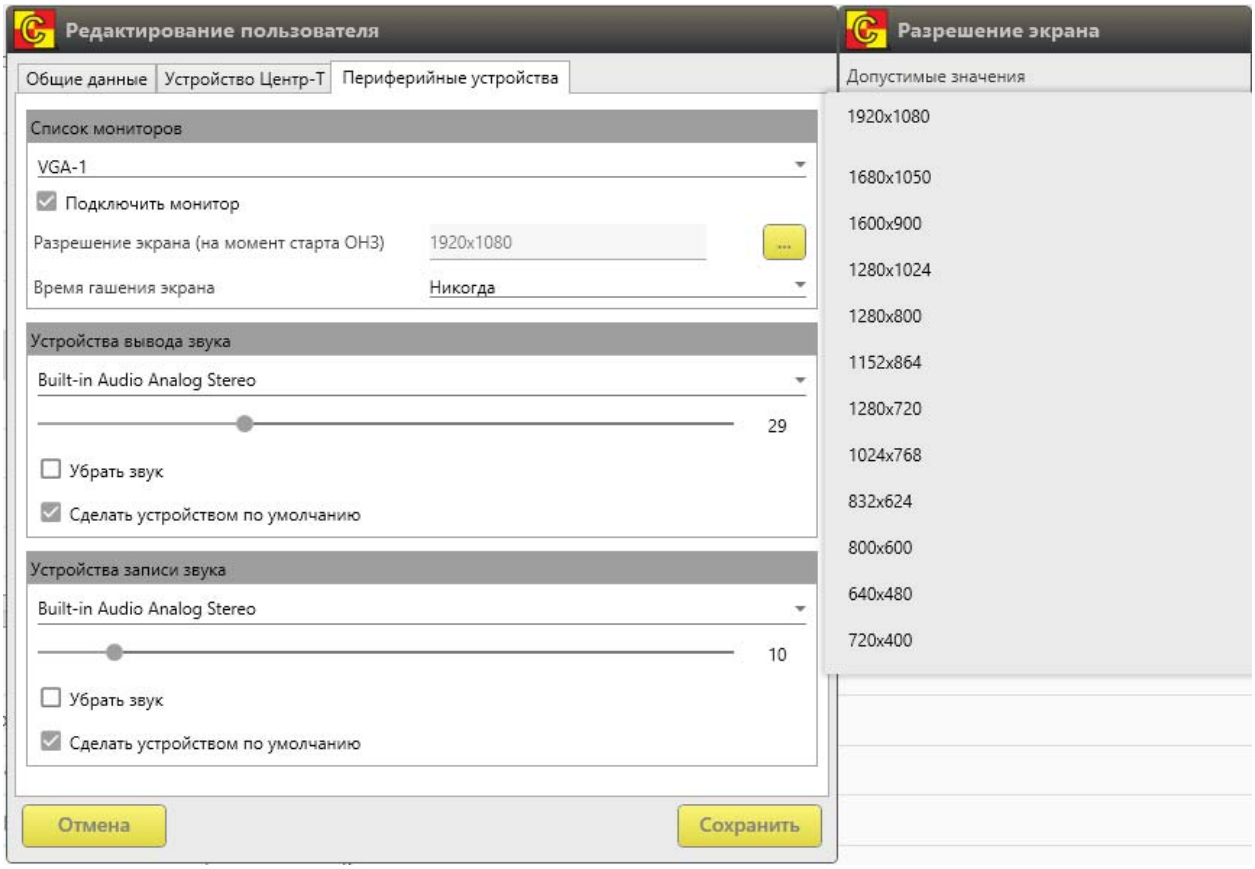


Рисунок 42 - Настройка разрешения экрана пользователя

Список мониторов пользователя и перечень доступных разрешений экрана для каждого из мониторов становятся доступными только после того, как пользователь хотя бы один раз войдет в систему.

ВНИМАНИЕ! При работе с терминалом HP510t возможна работа только с одним монитором. Подробнее см. Приложение 3 настоящего документа.

4.5.2.2. Настройка параметров кэширования

Для каждого клиентского устройства Администратор СХСЗ может задавать следующие настройки (рисунок 40):

– «Кэшировать образ» – позволяет включить/выключить функцию сохранения образа на клиентском устройстве после первого обращения к СХСЗ на получение образа (необязательный параметр). В случае установки этого флага с СХСЗ будет скачиваться только измененная часть образа (при ее наличии);

– «Удалять кэш образов при следующем включении (однократная операция)» – позволяет удалить все кэшированные образы в случае, если заканчивается место на клиентском устройстве.

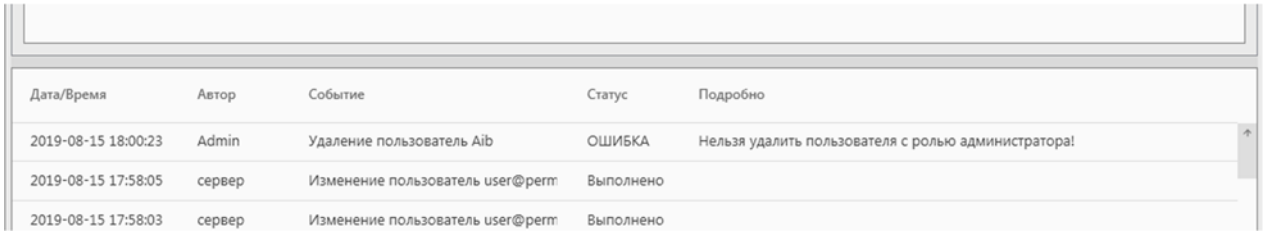
ВНИМАНИЕ! При использовании Клиента версий 1.2.6 – 1.2.11, на котором были кэшированы образы, полученные от СХСЗ версий 1.2.6 - 1.2.11, с СХСЗ версии 1.3.0 при установке подключения произойдет скачивание переназначенных соответствующих образов. При необходимости использования Клиентов версий 1.2.6 - 1.2.11 с СХСЗ версии 1.3.0 для корректной работы рекомендуется установить параметр «Удалять кэш образов при следующем включении (однократная операция)» соответствующему пользователю клиентского устройства. Указанный параметр позволит очистить информацию об образах на Клиенте, и при последующих подключениях будет использоваться кэшированный образ от СХСЗ версии 1.3.0.

4.5.3. Удаление учетных записей

Чтобы удалить учетную запись, необходимо в главном окне ПО управления СХСЗ перейти на вкладку «Пользователи», выбрать в таблице записи пользователей, которые следует удалить, и нажать клавишу «del» или вызвать контекстное меню по нажатию правой кнопкой мыши и выбрать команду «Удалить».

Администратор СХСЗ может удалять только те учетные записи, для которых установлена роль «Пользователь клиентского устройства». Если учетной записи присвоена роль административной группы, следует сначала назначить ей роль пользователя клиентского устройства (выполняется Администратором БИ или Администратором НШР) и только затем – удалить.

При попытке удалить учетные записи с ролью администратора удаленного управления СХСЗ возникнет ошибка «Нельзя удалить пользователя с ролью администратора!» (рисунок 43).



Дата/Время	Автор	Событие	Статус	Подробно
2019-08-15 18:00:23	Admin	Удаление пользователь Aib	ОШИБКА	Нельзя удалить пользователя с ролью администратора!
2019-08-15 17:58:05	сервер	Изменение пользователь user@perm	Выполнено	
2019-08-15 17:58:03	сервер	Изменение пользователь user@perm	Выполнено	

Рисунок 43 - Сообщение об ошибке «Нельзя удалить пользователя с ролью администратора!»

4.5.4. Экспорт пользователей в файл .csv

Для экспорта пользователей в файл .csv необходимо на вкладке «Пользователи» отметить одного или нескольких пользователей, правой кнопкой мыши вызвать контекстное меню и выбрать в нем команду «Экспорт». Откроется окно выбора параметров для выгрузки (рисунок 44). В этом окне уже отмечены и недоступны для изменения обязательные параметры экспорта (логин, ФИО, роль, SN устройства, последнее включение), но имеется возможность выбора дополнительных параметров. В строке «Файл» при нажатии кнопки ... в конце строки следует указать путь к файлу .csv и его имя. После того как выбранный файл отобразится в этой строке, кнопкой <Выполнить> можно запустить процесс выгрузки списка пользователей. При успешном завершении этого процесса появляется соответствующее информационное сообщение (рисунок 45).

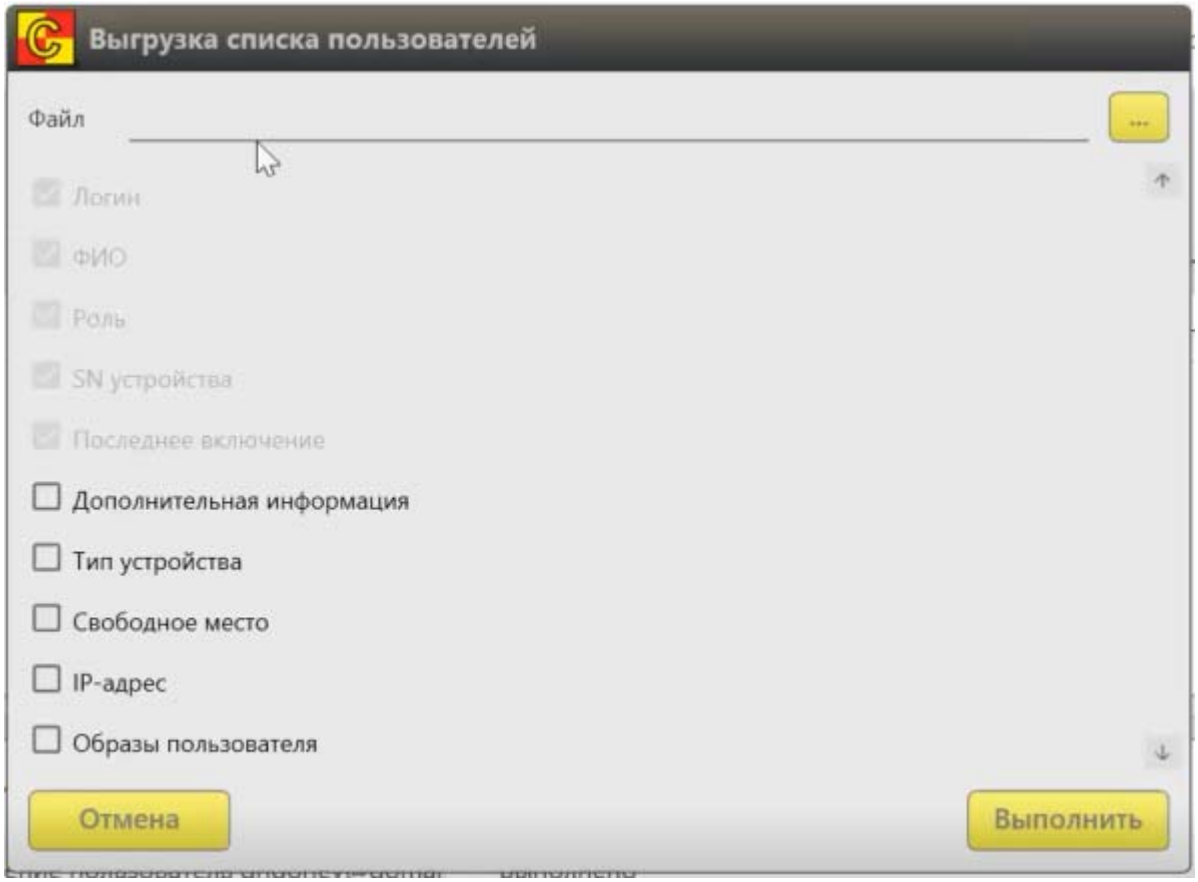


Рисунок 44 – Окно параметров экспорта списка пользователей

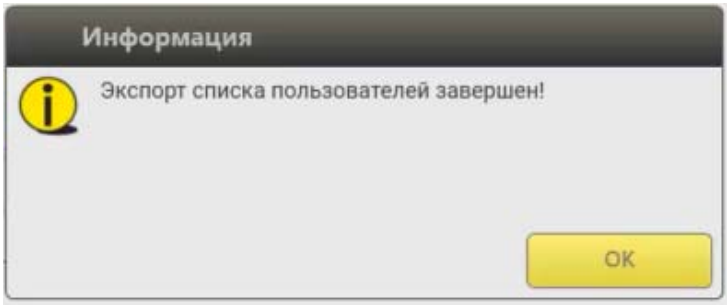


Рисунок 45 – Сообщение об успешном экспорте пользователей

4.6. Задание параметров терминала пользователя

На вкладке «Периферийные устройства» окна «Редактирование пользователя» (рисунок 46) можно задать следующие параметры терминала пользователя:

- настройки мониторов (блок «Список мониторов»), при этом для каждого монитора из выпадающего списка задаются:
  - подключение (параметр «Подключить монитор»)
  - разрешение экрана на момент старта ОНЗ (задается при нажатии на кнопку ...);

- время гашения экрана (задается в раскрывающемся списке значением от 1 минуты до 5 часов или «Никогда»);

– настройки устройств вывода и записи звука (блоки «Устройства вывода звука» и «Устройства записи звука» соответственно), при этом для каждого устройства из выпадающего списка задаются:

  - громкость (ползунок, позволяющий изменить значение параметра в диапазоне от 0 до 100);
  - отключение (параметр «Убрать звук»);
  - использование в качестве устройства по умолчанию (параметр «Сделать устройством по умолчанию»).

При снятии флага «Подключить монитор» следует учесть, что все мониторы рабочей станции отключить нельзя, и при попытке убрать флаг с единственного подключенного монитора появится предупреждение о невозможности данного действия (рисунок 47).

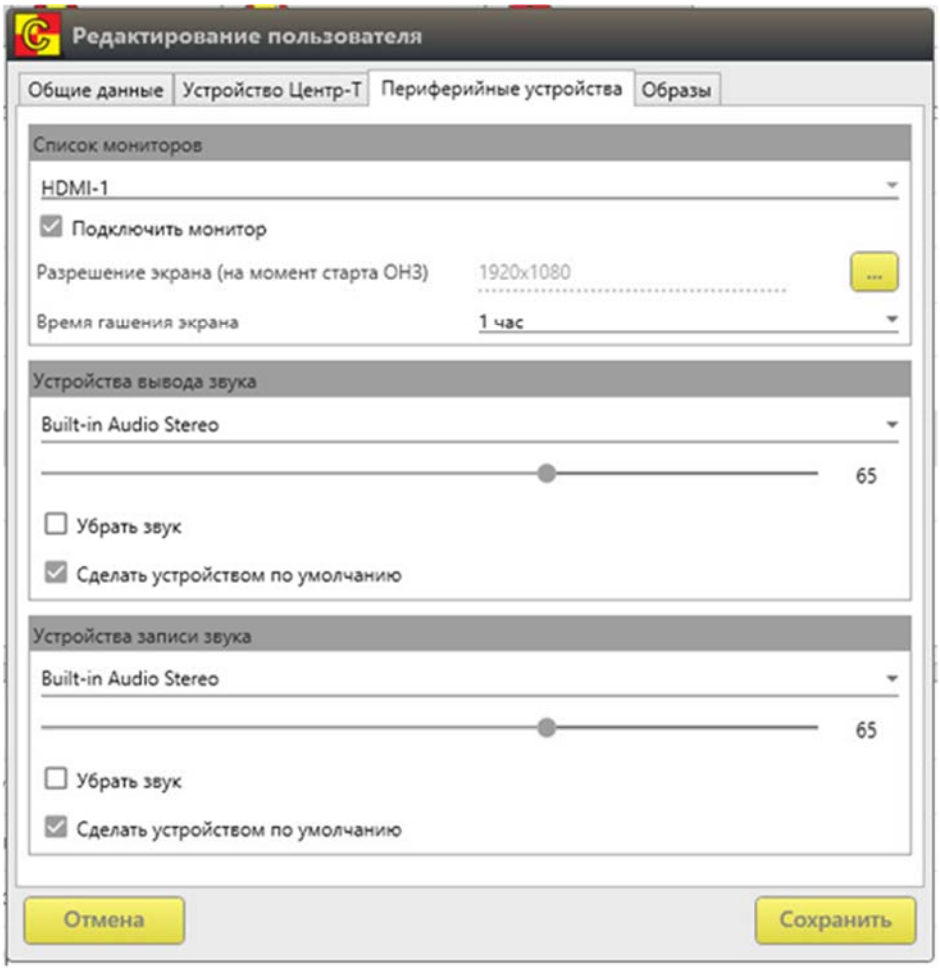


Рисунок 46 - Вкладка «Периферийные устройства» окна «Редактирование пользователя»

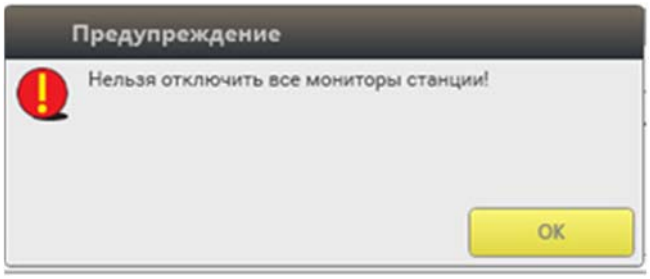


Рисунок 47 – Предупреждение о невозможности отключения всех мониторов станции

4.7. Просмотр информации о терминалах пользователей

Администратор СХСЗ может просматривать информацию о терминалах пользователей после их загрузки со специального носителя, назначенного Администратором БИ пользователю. Подробнее о просмотре информации об оборудовании пользователей см. п.5.9.

4.8. Управление шаблонами настроек образов ПО ТС

4.8.1. Создание шаблона настроек образа

Шаблоны настроек содержат изменяемые параметры образа ПО ТС и могут использоваться для нескольких образов.

Для создания шаблона настроек образа необходимо перейти на вкладку «Управление шаблонами» и нажать правой кнопкой мыши в любом месте таблицы шаблонов.

После этого появляется окно создания шаблона настроек (рисунок 48).

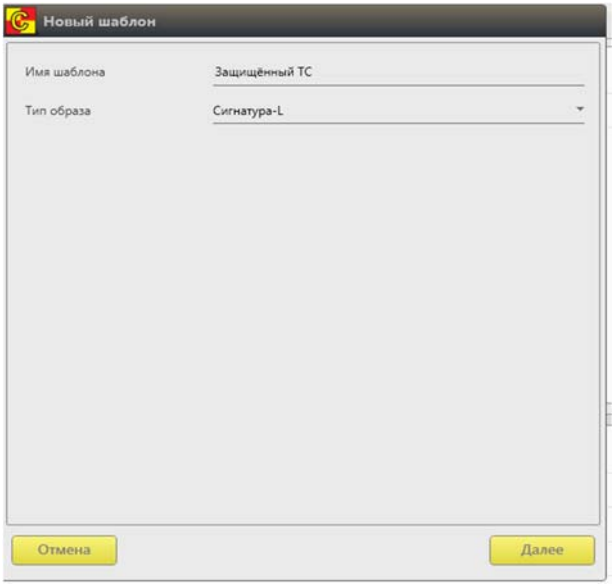


Рисунок 48 - Окно создания шаблона настроек

В первую очередь следует указать уникальное имя шаблона и выбрать из выпадающего списка тип: Citrix (обычный для соединения по

протоколу ICA) или Сигнатура-L (с возможностью работы со СКАД «Сигнатура-L»).

Рекомендуется указывать в качестве имени строку, отражающую суть задаваемых в шаблоне параметров, так как имя шаблона будет в дальнейшем отображаться Пользователям клиентского устройства.

Нажать кнопку «Далее».

Для шаблона образа Citrix (обычное соединение по протоколу ICA) необходимо указать только адрес брокера Citrix[5] (IP или FQDN), один или несколько. Для добавления адреса нажмите на кнопку ..., а затем правой кнопкой мыши по пустой области появившейся таблицы «IP». Выберите в выпадающем меню пункт «Добавить», после чего заполните появившуюся строку таблицы и нажмите клавишу «Enter» (рисунок 49).

Рисунок 49 - Добавление адресов в шаблон образа Citrix

Аналогичным образом добавьте все требуемые адреса в таблицу, после чего нажмите кнопку «Завершить». Заданные адреса будут отображены в строке «Брокер (IP/FQDN)» (рисунок 50).

[5] Сведения справочного характера по настройке страницы Autologin для образов с поддержкой SSO приведены в Приложении 1.

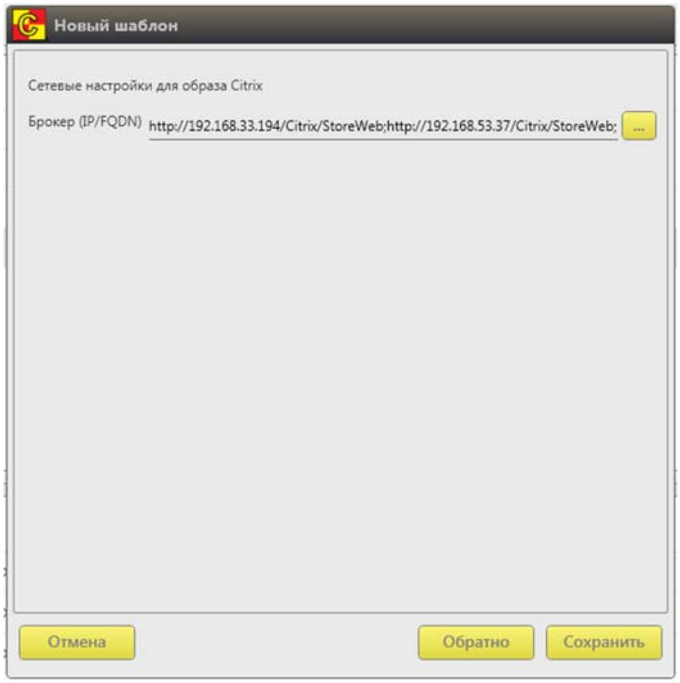


Рисунок 50 - Отображение заданных адресов в строке «Брокер (IP/FQDN)»

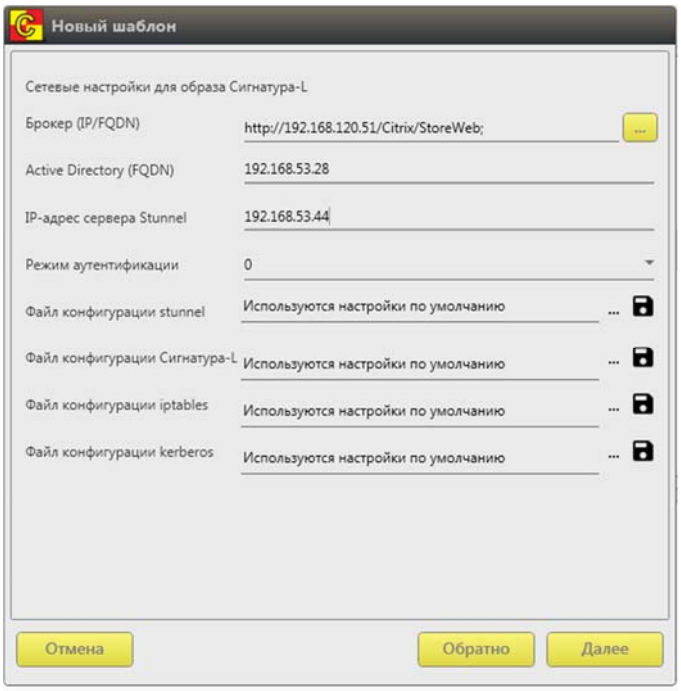


Рисунок 51 - Расширенные настройки для образа «Сигнатура-L»

Для образа с возможностью работы со СКАД «Сигнатура-L», помимо задания адреса брокера Citrix (IP или FQDN), требуются расширенные настройки (рисунок 51):

– «Брокер» – позволяет задать адрес брокера (обязательный параметр), один или несколько;

– «Active Directory» – позволяет задать адрес сервера службы AD (обязательный параметр);

– «IP-адрес stunnel server» – позволяет задать адрес сервера stunnel в сети (обязательный параметр);

– «Режим аутентификации» – позволяет задать режим аутентификации из выпадающего списка (параметр verify в stunnel.desktop.conf);

– «Файл конфигурации stunnel» – позволяет загрузить файл конфигурации stunnel (обязательный параметр; если не указывается Администратором БИ вручную, используется заданный по умолчанию файл). В случае установки флага «Использовать proxy-сервер» данный файл конфигурации должен быть изменен так, как описано ниже;

– «Файл конфигурации Сигнатура-L» – позволяет загрузить файл конфигурации Сигнатура-L (обязательный параметр; если не указывается Администратором БИ вручную, используется заданный по умолчанию файл);

– «Файл кофигурации iptables» – позволяет загрузить файл конфигурации iptables (обязательный параметр; если не указывается Администратором БИ вручную, используется заданный по умолчанию файл). В случае установки флага «Использовать proxy-сервер» данный файл конфигурации должен быть изменен так, как описано ниже;

– «Файл конфигурации kerberos» – позволяет загрузить файл конфигурации kerberos (обязательный параметр; если не указывается Администратором БИ вручную, используется заданный по умолчанию файл);

– «Использовать proxy-сервер» (рисунок 52) – позволяет включить/ выключить поддержку proxy-сервера Squid (необязательный параметр; требуется, если планируется использование proxy-сервера Squid). После установки флага становятся доступны строки для указания сетевых параметров, необходимых для взаимодействия proxy-сервера с клиентом stunnel:

– «IP-адрес» – позволяет задать сетевой адрес proxy-сервера, указанный в настройках браузера (обычно 127.0.0.1);

– «Порт» – позволяет задать свободный локальный порт клиента stunnel, на котором он принимает трафик и с которого передает трафик на сервер stunnel;

– Дополнительные параметры настройки stunnel:

– «IP назначения» – позволяет задать адрес сервера Citrix, на который следует отправлять данные с клиентского устройства через сервер stunnel (не обязательный параметр; требуется, если ip-адрес назначения не указан в файлах настроек);

– «Порт назначения» – позволяет задать порт сервера Citrix, на который следует отправлять данные с клиентского устройства

через сервер stunnel (не обязательный параметр; требуется, если порт назначения не указан в файлах настроек);

– «Локальный порт» – позволяет задать порт клиента stunnel, на котором он принимает трафик и с которого передает трафик на сервер stunnel (не обязательный параметр; требуется, если локальный порт не указан в файлах настроек);

– «Порт stunnel» – позволяет задать порт сервера stunnel, который принимает данные с клиентского устройства (не обязательный параметр; требуется, если порт stunnel не указан в файлах настроек).

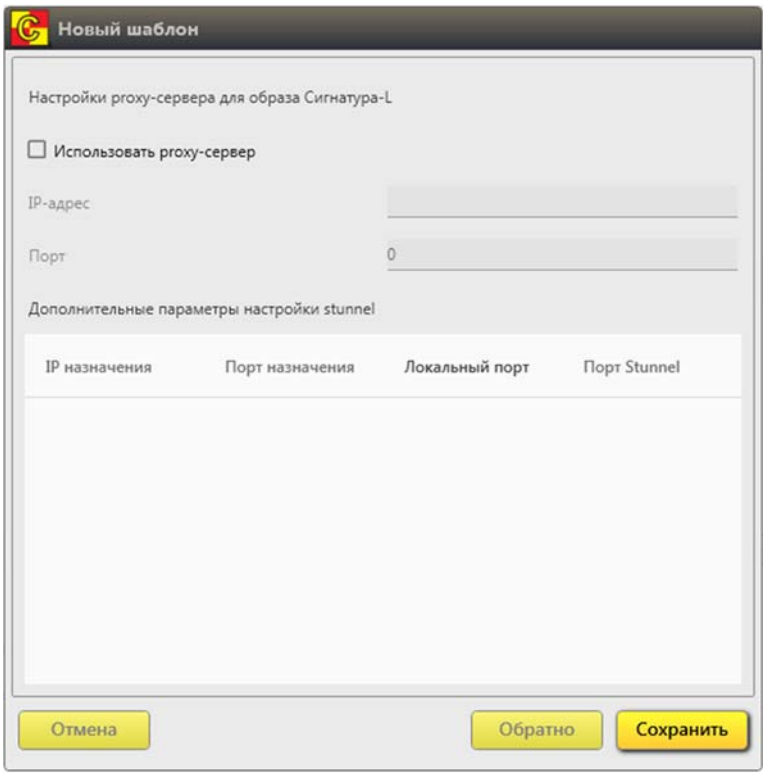


Рисунок 52 - Настройки proxy-сервера для образа «Сигнатура-L»

Сохранение шаблона с заданными параметрами осуществляется по кнопке <Сохранить>.

Созданный шаблон появится в таблице во вкладке «Шаблоны».

В случае использования proxy-сервера помимо выполнения указанных настроек в ПО Клиента следует дополнительно:

1) весь трафик в подсети, в которой находятся proxy-сервер Squid и брокер Citrix, перенаправить с помощью iptables на любой свободный порт клиента stunnel;

2) с помощью клиента stunnel с порта, используемого на шаге 1, перенаправить трафик на сервер stunnel, с которого он будет перенаправлен на proxy-сервер.

Для выполнения описанных дополнительных настроек необходимо:

– скачать текущие файлы конфигурации stunnel (stunnel.desktop.conf) и iptables (firewall.conf) по нажатию кнопки в строках «файл конфигурации stunnel» и «файл конфигурации iptables» соответственно (рисунок 51);

– открыть файл stunnel.desktop.conf, используя текстовый редактор[6] из комплекта поставки продукта, и произвести следующие изменения: заменить строку %(proxy_rules)s записью

[Rule 0]

client = yes

accept = 0.0.0.0:[port1]

connect = [ipStunnel]:[port2],

где *[ipStunnel]* – ip-адрес сервера stunnel, *[port1]* – свободный локальный порт клиента stunnel, на котором он принимает трафик и с которого передает трафик на сервер stunnel, *[port2]* – порт сервера stunnel, на котором он принимает трафик от клиента stunnel и с которого будет направлять трафик на прокси-сервер Squid;

– открыть файл firewall.conf, используя текстовый редактор, и произвести следующие изменения: заменить строку %(iptables_rules)s записью

-A OUTPUT -d [netaddr]/[mask] -p tcp -m tcp -j DNAT --match multiport --dports 80,1494,2598 --to-destination 127.0.0.1:[port1],

где *[netaddr]* – адрес сети, *[mask]* – маска сети, в которой работает Squid и брокер Citrix; *[port1]* – локальный порт клиента stunnel, указанный на шаге 1 и в строке «Порт»; 80, 1494, 2598 – номера портов клиента stunnel, на которые перенаправляется трафик. Пример записи:

-A OUTPUT -d 192.168.53.0/24 -p tcp -m tcp -j DNAT --match multiport --dports 80,1494,2598 --to-destination 127.0.0.1:10002.

Полученные в результате файлы stunnel.desktop.conf и firewall.conf следует использовать при создании шаблона с поддержкой СКАД «Сигнатура-L».

ВНИМАНИЕ! При использовании шаблонов с поддержкой СКАД «Сигнатура-L» может возникнуть необходимость отключения использования сетевого справочника сертификатов. Для выполнения операции необходимо скачать текущий файл конфигурации СКАД

[6] Для внесения изменений в файлы конфигурации может использоваться не любой текстовый редактор. Например, использование стандартного средства Windows «Блокнот» ведет к получению некорректного варианта файла (при просмотре такого файла в hex можно увидеть, что в начале добавляется EF - Byte Order Mark. Stunel в Linux обрабатывает такие файлы некорректно). По этой причине для правки файлов конфигурации рекомендуется использовать текстовый редактор из комплекта поставки «Центр-Т» либо иной текстовый редактор, использование которого не приводит к описанному эффекту.

«Сигнатура-L» по нажатию кнопки в строке «файл конфигурации Сигнатура-L». Далее следует открыть скачанный файл (с расширением .spki) с помощью текстового редактора и произвести изменения: в секции [Profile_0] заменить строку «Count = 3» на «Count = 2» и удалить строку, в которой указан сетевой справочник.

Полученный в результате файл следует использовать при создании шаблона с поддержкой СКАД «Сигнатура-L».

4.8.2. Редактирование шаблона настроек образа

Созданные шаблоны настроек образа ПО ТС можно изменить. Для этого необходимо перейти на вкладку «Управление шаблонами», выбрать шаблон, который планируется изменить, и нажать клавишу «Enter» или вызвать команду "Редактировать" из контекстного меню.

После выполнения всех изменений нужно нажать кнопку <Сохранить>.

4.8.3. Удаление шаблона настроек образа

Если шаблон настроек образа не используется, его можно удалить. Для этого нужно на вкладке «Управление шаблонами» выбрать удаляемый шаблон и нажать клавишу «del» или вызвать команду «Удалить» из контекстного меню.

4.9. Просмотр событий безопасности

Администратор СХСЗ может просматривать события безопасности:

- собственной сессии;
- сессий администраторов удаленного управления СХСЗ;
- сессий пользователей клиентских устройств.

Все события фиксируются в общем журнале и отображаются на вкладке «Журнал событий» (рисунок 53).

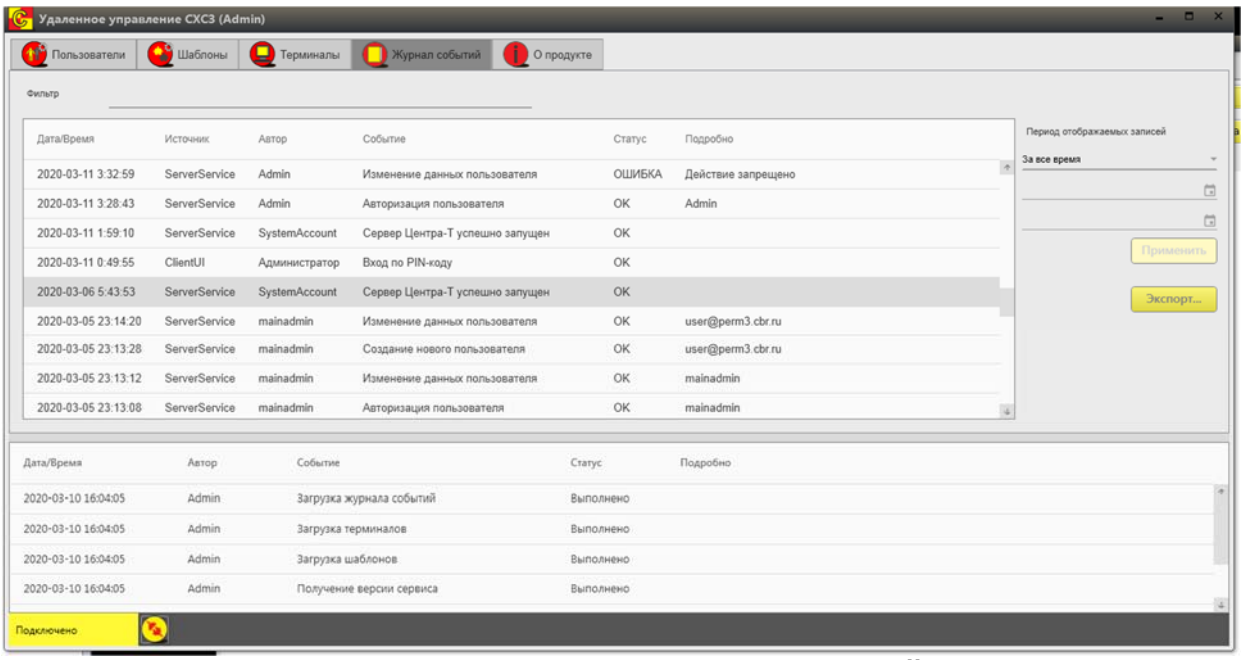


Рисунок 53 - Вкладка «Журнал событий»

События текущей сессии отображаются в нижней части окна вкладки «Журнал событий».

Общий журнал хранится в БД (внутренней или внешней, в зависимости от настроек СХСЗ) и не перезаписывается при выключении или перезагрузке как СХСЗ, так и внешней СУБД.

Для поиска нужной информации в событиях можно использовать функцию фильтра, доступную в верхней части окна. Применение фильтра происходит при нажатии на клавишу «Enter», поиск осуществляется с учетом регистра. Для удаления фильтра необходимо удалить искомый текст и вновь нажать клавишу «Enter».

Также есть возможность просмотра события за определенный период. Для использования этой функции нужно выбрать период отображаемых записей в правой части окна и нажать кнопку <Применить>. Доступны следующие варианты:

- за сегодня (по умолчанию);
- за предыдущий день;
- за неделю;
- за месяц;
- за указанный (произвольный) период.

ВНИМАНИЕ! События, отображаемые в журнале, указаны по текущему времени на рабочем месте Администратора СХСЗ, на котором установлена утилита удаленного управления, при этом фильтры по временному периоду работают со временем событий в UTC.

При нажатии кнопки <Экспорт> доступна функция экспорта журнала событий. Экспорт записей производится в соответствии с

заданным фильтром по времени в текстовом формате в файл с расширением .txt.

4.10. Восстановление сессии пользователя

В статусной строке главного окна программы удаленного управления СХСЗ отображается индикатор наличия связи с сервером RMQ – желтая надпись «Подключено». Рядом с ней располагается кнопка для проверки подключения.

Рисунок 54 – Статус «Подключено»

Если в процессе работы происходит потеря связи с сервером RMQ, цвет индикатора меняется на серый, а сообщение – на «Связь потеряна».

Рисунок 55 – Статус «Связь потеряна»

Если связь будет восстановлена, то программа автоматически возобновит подключение. Пользователь может проверить наличие подключения вручную, кликнув по кнопке <Проверить подключение>.

В случае потери связи пользователь может просматривать данные, но не может выполнять никаких операций добавления, удаления или редактирования.

4.11. Просмотр информации о продукте и статусе лицензии СХСЗ

Администратор СХСЗ может просматривать информацию о продукте, а также о статусе лицензии СХСЗ. Для этого следует перейти на вкладку «О продукте» в ПО управления СХСЗ (рисунок 56).

Доступна следующая информация о продукте:

- наименование продукта;
- версия продукта;
- версия АРМ удаленного управления;
- версия сервиса ПО удаленного управления;
- производитель;
- контакты производителя.

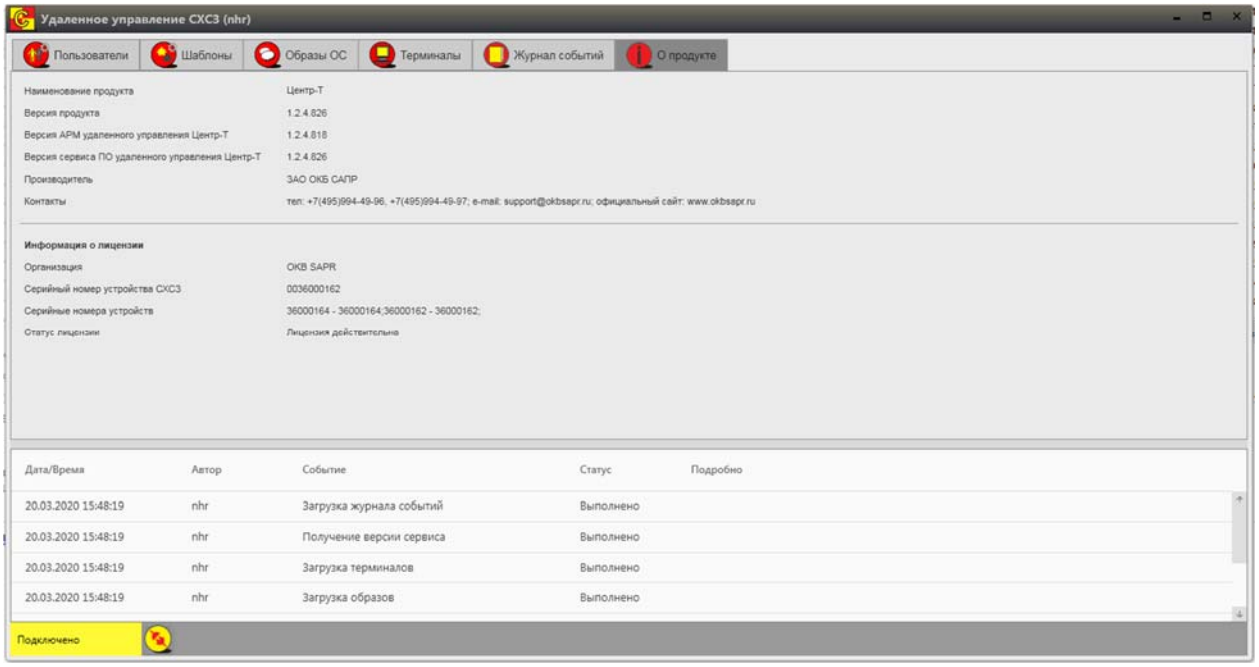


Рисунок 56 – Информация о продукте

Также доступна информация о статусе лицензии СХСЗ:

- имя организации (имя организации, на которую выписана указанная лицензия);
- тип сервера (начиная с версии 1.2.10, рисунок 57);

- серийный номер устройства СХСЗ (серийный номер носителя, с которого загружен СХСЗ);
- серийные номера устройств (серийные номера, на которые выписана используемая лицензия);
- статус лицензии (если недействительна, то указана причина).

Информация о лицензии	
Организация	OKB SAPR
Тип сервера:	Виртуальный сервер
Серийный номер устройства СХСЗ	0036000003
Серийные номера устройств	36000003 - 36000003;
Статус лицензии	Лицензия действительна

Рисунок 57 – Информация о статусе лицензии СХСЗ версии 1.2.10

Также в нижней строке ПО сервисного режима работы СХСЗ доступна информация о версиях ОНЗ и СХСЗ сервиса ПО удаленного управления Центр-Т.

4.12. Завершение работы ПО управления

Для завершения работы Администратор должен нажать кнопку ✕ в ПО управления СХСЗ и завершить работу с ПО удаленного доступа к СХСЗ.

5. Состав работ Администратора безопасности информации

5.1. Общие сведения

Если планируется использование учетных записей администраторов удаленного управления, созданных по умолчанию, Администратор БИ может начать выполнение своих функциональных обязанностей после того, как Администратор сервисного режима установил сетевые настройки СХСЗ и подключил внешний носитель с образами ПО ТС. В соответствии со своими обязанностями Администратор БИ должен:

1) установить ПО для получения удаленного доступа (см. 5.2);

2) получить доступ к ПО управления СХСЗ (см. 5.3), используя учетную запись, созданную по умолчанию;

3) изменить пароль Администратора БИ и назначить собственный идентификатор (процедура выполняется принудительно при первом входе) (см. 5.4).

Если планируется использование учетных записей администраторов удаленного управления, созданных при настройке СХСЗ, Администратор БИ может начать выполнение своих функциональных обязанностей после того, как Администратор создал две учетные записи, предназначенные для администраторов удаленного управления. В этом случае Администратор БИ должен:

1) получить доступ к ПО управления СХСЗ (см.5.3), используя учетную запись, созданную по умолчанию;

2) назначить новым учетным записям роли администраторов удаленного управления СХСЗ, задав им пароль (собственной учетной записи Администратор БИ дополнительно должен назначить идентификатор) (см. 5.7);

3) получить доступ к ПО управления СХСЗ (см.5.3), используя новую учетную запись Администратора БИ.

После выполнения Администратором СХСЗ процедуры создания учетных записей пользователей Администратор БИ СХСЗ, получив журнал, в котором серийные номера клиентских устройств соотнесены с ФИО пользователей:

1) назначает пользователям клиентские устройства (см.5.8);

2) назначает пользователям образы ПО ТС (см. 5.10) (опционально может быть целесообразным фиксировать в собственном журнале соответствие серийных номеров клиентских устройств ФИО пользователей);

3) просматривает информацию об используемом оборудовании пользователей (см.5.9);

4) создает шаблоны настроек ПО ТС и назначает их пользователям (см. 5.10).

В процессе эксплуатации Комплекса Администратор БИ может выполнять смену роли учетной записи (см. 5.7), изменять собственные параметры идентификации (см. 5.4), осуществлять экспорт списка пользователей (5.11) и получать доступ к журналам регистрации событий (см. 5.12).

5.2. Установка ПО для удаленного доступа к СХСЗ

Установка ПО для удаленного доступа к СХСЗ выполняется Администратором на собственном АРМ так же, как и для Администратора СХСЗ (см. 4.2).

5.3. Получение доступа к ПО управления СХСЗ

Процедура получения доступа Администратора БИ к ПО управления СХСЗ выполняется в целом так же, как и аналогичная процедура для Администратора (см. 4.3). Отличие состоит в том, что Администратор БИ использует собственные параметры идентификации. Для первого входа это параметры, установленные по умолчанию – логин aib и пароль P@ssw0rd (если идентификатор подключен в этот момент к СВТ, то он будет проигнорирован при первом входе). При первом входе в ПО управления СХСЗ выполняется принудительное изменение пароля и назначение собственного идентификатора. Порядок выполнения процедуры назначения устройства и нового пароля указан в пункте 5.4. В дальнейшем смена пароля/идентификатора может быть произведена в любое время.

Все последующие действия должны выполняться от имени той учетной записи, которую планируется использовать для работы с СХСЗ.

Если идентификация Администратора БИ выполнена успешно, появляется главное окно ПО управления СХСЗ с доступными Администратору БИ настройками (рисунок 58).

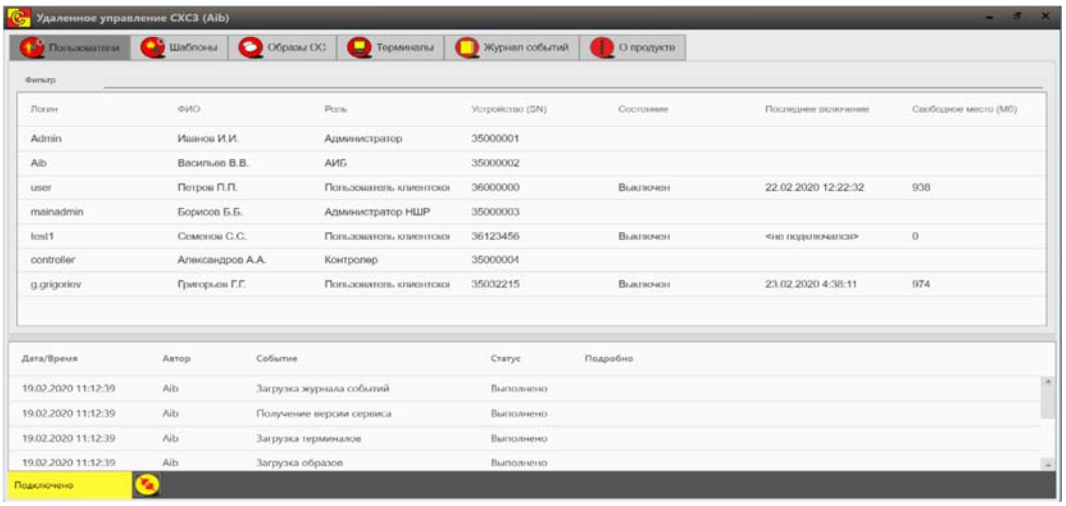


Рисунок 58 - Главное окно ПО управления СХСЗ

Учетная запись, от имени которой работает Администратор БИ, указана в строке с названием утилиты.

5.4. Изменение параметров идентификации Администратора безопасности информации

Для идентификации Администратор БИ использует пароль и отчуждаемое аппаратное устройство.

Для изменения параметров идентификации Администратору БИ необходимо перейти на вкладку «Пользователи» в главном окне ПО управления СХСЗ и выбрать собственную учетную запись. Далее по щелчку правой кнопкой мыши следует вызвать окно доступных действий и выбрать пункт «Редактировать». При этом появляется окно настроек учетной записи Администратора БИ (рисунок 59). В появившемся окне нужно ввести старый пароль и новый пароль Администратора БИ с подтверждением, если требуется сменить пароль; если необходимо назначить/изменить идентификатор Администратора БИ, то следует подключить и выбрать в списке новое устройство.

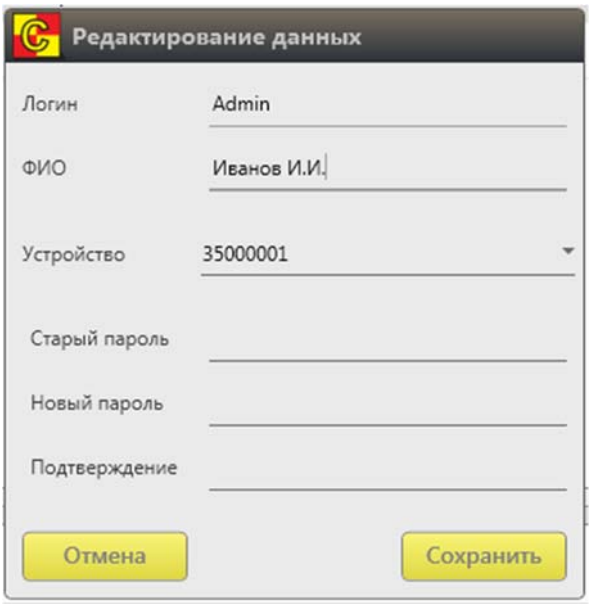


Рисунок 59 - Окно настройки учетной записи Администратора БИ

Сохранение параметров идентификации Администратора БИ выполняется по кнопке <Сохранить>. После выполнения необходимых настроек следует перезапустить утилиту.

5.5. Просмотр образов ПО ТС

Текущие образы ПО ТС отображены на вкладке «Образы ОС» (рисунок 60).

В зависимости от архитектуры терминала пользователя доступны следующие образы:

а) для работы на терминалах с архитектурой X86-64[7]:

- образы с возможностью проброса USB-устройств в терминальную сессию:

– образ для работы по протоколу ICA, допускающий наличие комплекса семейства «Аккорд» на терминальном сервере (citrix_18_10-vc);

– образ для работы по протоколу ICA, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_18_10-vc-sso);

– образ, поддерживающий работу со СКАД Сигнатура-L, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_18_10-vc-sso-stunnel_6_0_480);

- образы без поддержки проброса USB-устройств в терминальную сессию:

– образ для работы по протоколу ICA, допускающий наличие комплекса семейства «Аккорд» на терминальном сервере (citrix_18_10-vc_nousb);

– образ для работы по протоколу ICA, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_18_10-vc-sso_nousb);

– образ, поддерживающий работу со СКАД Сигнатура-L, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_18_10-vc-sso-stunnel_6_0_480_nousb);

б) для работы на Защищенном терминале Центр-TrusT с архитектурой ARM64:

- образы с возможностью проброса USB-устройств в терминальную сессию:

– образ для работы по протоколу ICA, допускающий наличие комплекса семейства «Аккорд» на терминальном сервере (citrix_13_10-vc-mtrust);

– образ для работы по протоколу ICA, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_13_10-vc-sso-mtrust);

- образы без поддержки проброса USB-устройств в терминальную сессию:

[7] Подробнее о работе Пользователя клиентского устройства в рамках терминальной сессии можно прочитать в п. 5.3 «Руководства по эксплуатации клиентских устройств»

– образ для работы по протоколу ICA, допускающий наличие комплекса семейства «Аккорд» на терминальном сервере (citrix_13_10-vc-mtrust_nousb);

– образ для работы по протоколу ICA, предполагающий наличие комплекса семейства «Аккорд» на терминальном сервере, а также поддерживающий технологию SSO (citrix_13_10-vc-sso-mtrust_nousb).

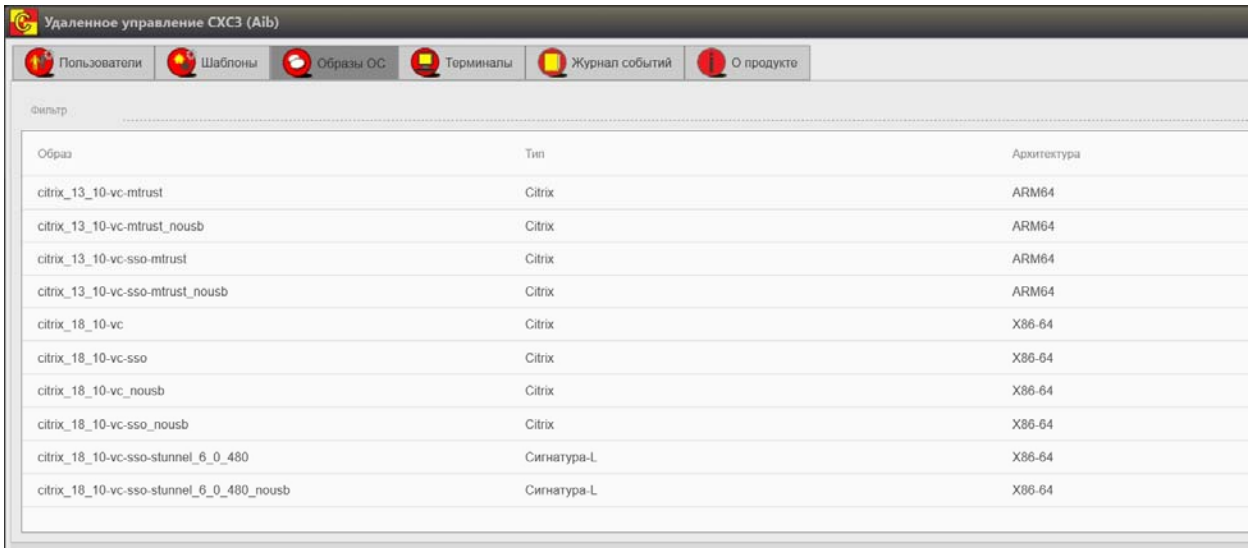


Рисунок 60 - Вкладка "Образы ОС"

5.6. Просмотр шаблонов настроек ПО ТС

Созданные Администратором СХСЗ или Администратором НШР шаблоны настроек ПО ТС доступны Администратору БИ для просмотра во вкладке «Шаблоны». В таблице для каждого шаблона указаны его имя и тип (рисунок 61).

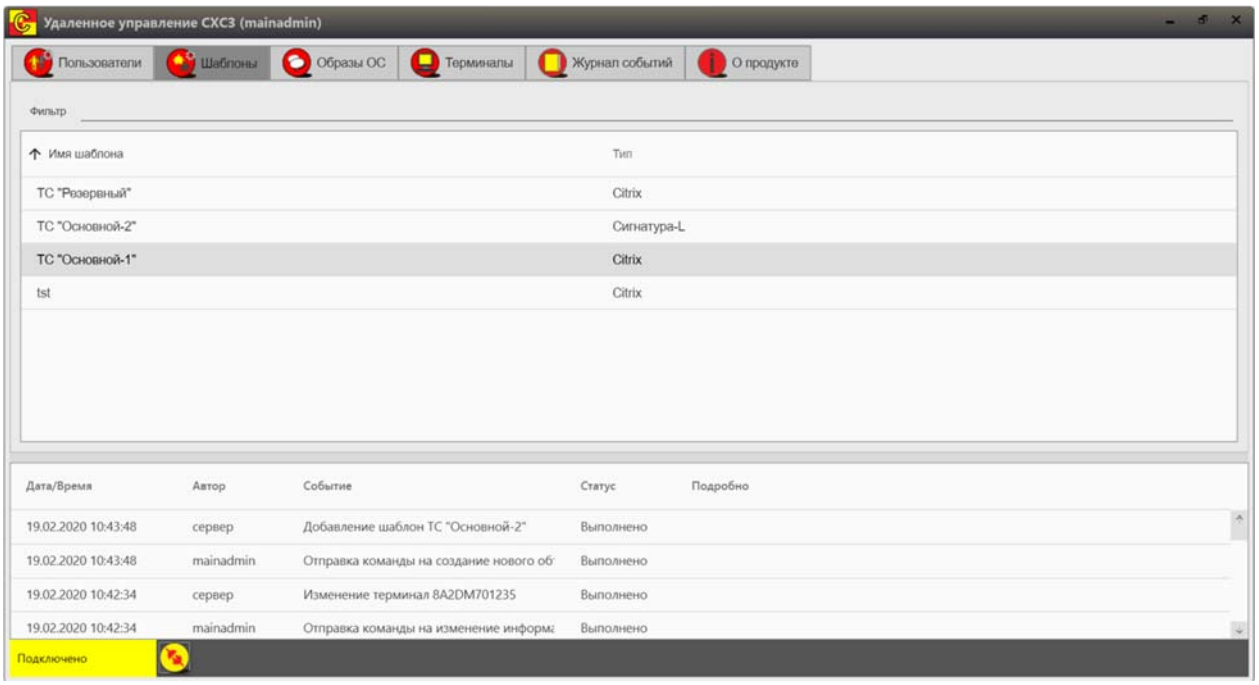


Рисунок 61 - Вкладка «Шаблоны» окна удаленного управления СХСЗ

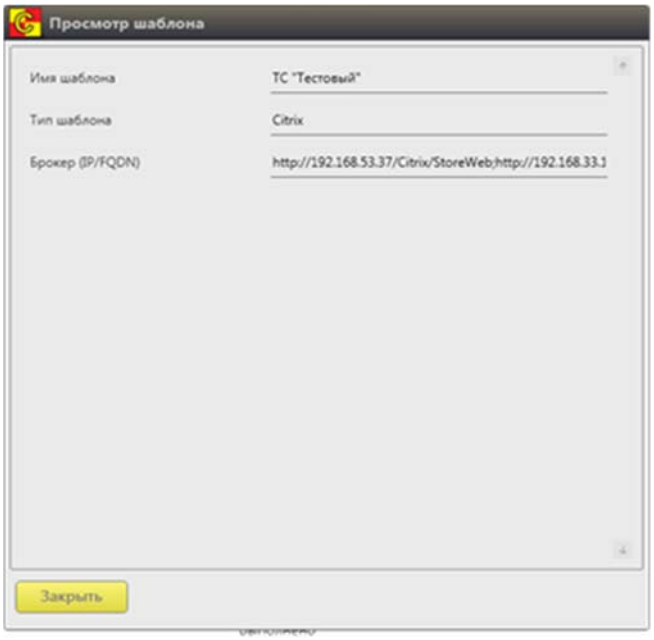


Рисунок 62 - Просмотр настроек шаблона

Для просмотра подробной информации следует нажать правой кнопкой мыши на шаблон и выбрать «Просмотр», после чего откроется окно с настройками, хранимыми в шаблоне (рисунок 62).

5.7. Редактирование настроек учетной записи пользователя

По умолчанию учетным записям присваивается роль «Пользователь клиентского устройства».

В некоторых случаях может понадобиться назначение учетной записи административной роли:

1) если планируется использование новых учетных записей администраторов удаленного управления СХСЗ, созданных в процессе эксплуатации ПАК «Центр-Т», вместо (помимо) учетных записей, созданных по умолчанию;

2) если необходимо создать резервные учетные записи администраторов удаленного управления (для доступа к функциям управления, если пароль существующей учетной записи одного из администраторов будет утерян).

Также возможны случаи, когда появляется необходимость присвоения учетной записи одного из администраторов роли обычного пользователя:

1) для получения возможности удаления учетной записи одного из администраторов, если она больше не требуется (есть резервная учетная запись с соответствующими административными правами);

2) при необходимости ограничения круга обязанностей должностного лица, выполняющего обязанности одного из администраторов удаленного управления (назначении другого сотрудника на роль Администратора, Администратора БИ, Администратора НШР или Контролера).

Для выполнения процедуры необходимо в главном окне ПО управления СХСЗ перейти на вкладку «Пользователи» (рисунок 63).

На этой вкладке для каждой учетной записи отображается следующая информация:

– логин;

– ФИО;

– роль;

– устройство (серийный номер);

– состояние: «Выключен» — если учетная запись в настоящий момент не используется, «Работает» — если используется, «Заблокирован» — если учетная запись заблокирована (только для учетных записей с ролью «Пользователь клиентского устройства»);

– последнее включение: дата и время последнего использования учетной записи (только для учетных записей с ролью «Пользователь клиентского устройства»);

– свободное место: объем свободной памяти на назначенном устройстве в момент старта ОНЗ (только для учетных записей с ролью «Пользователь клиентского устройства»).

Для редактирования учетной записи нужно выбрать ее в таблице и нажать клавишу «Enter» или вызвать команду «Редактировать» из контекстного меню.

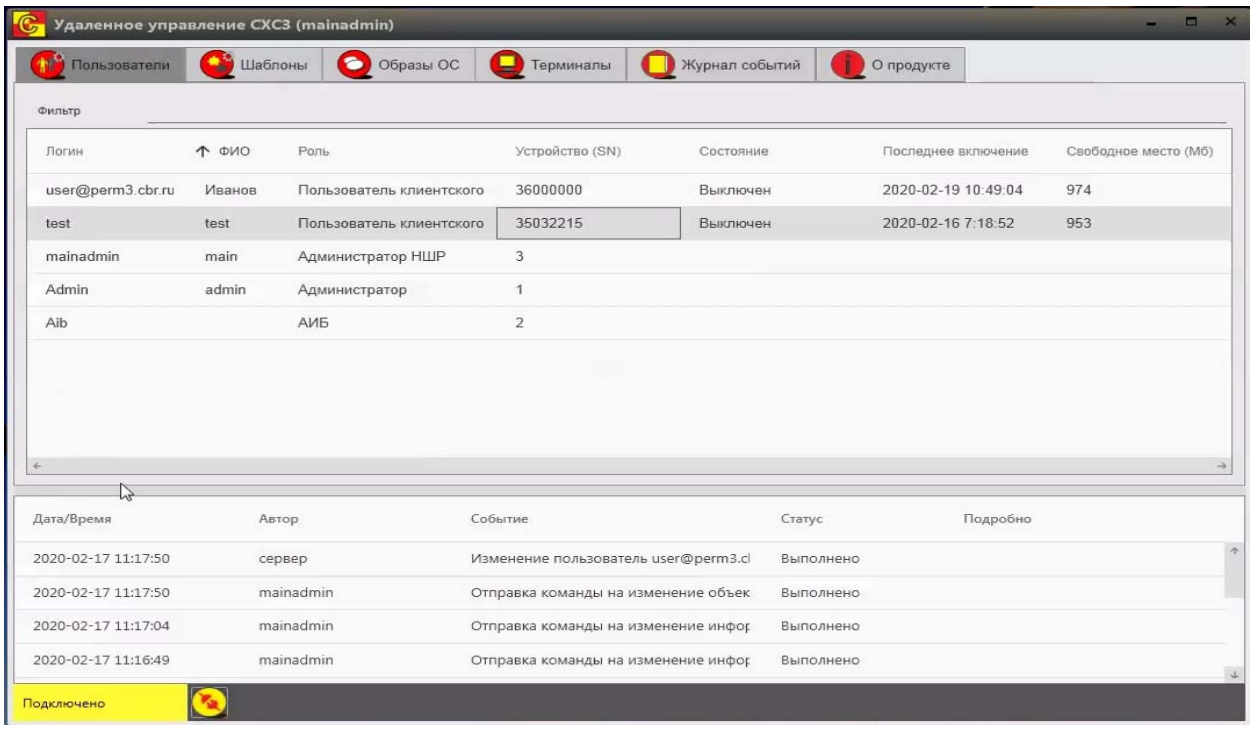


Рисунок 63 – Вкладка «Пользователи»

Появляется окно редактирования настроек учетной записи. Перечень доступных настроек отличается для учетной записи пользователя клиентского устройства (рисунок 65) и учетных записей администраторов удаленного управления СХСЗ (рисунок 64). Для администраторов доступны только смена роли и заполнение поля «Дополнительно».

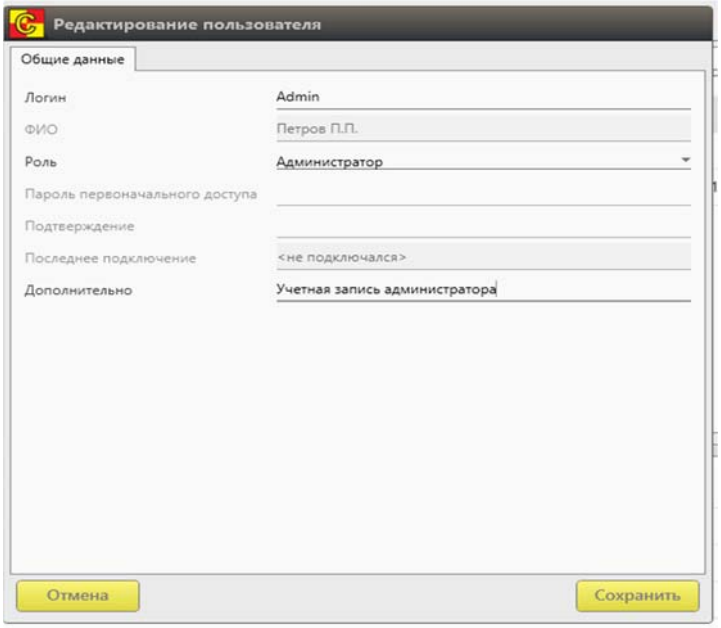


Рисунок 64 - Окно редактирования настроек учетной записи администраторов удаленного управления СХСЗ

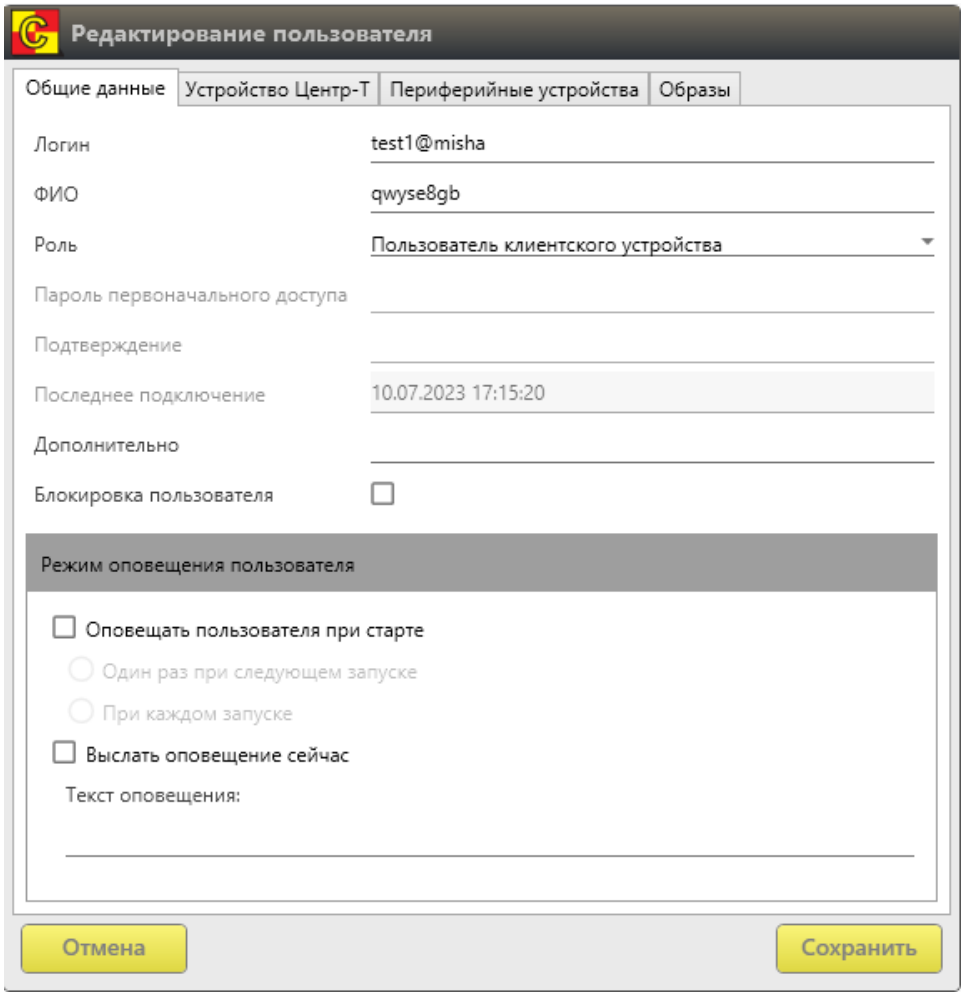


Рисунок 65 – Окно редактирования настроек учетной записи пользователя

Чтобы назначить новую роль учетной записи, следует в строке «Роль» выбрать соответствующую роль в выпадающем списке (рисунок 66) и далее задать некоторые параметры учетной записи.

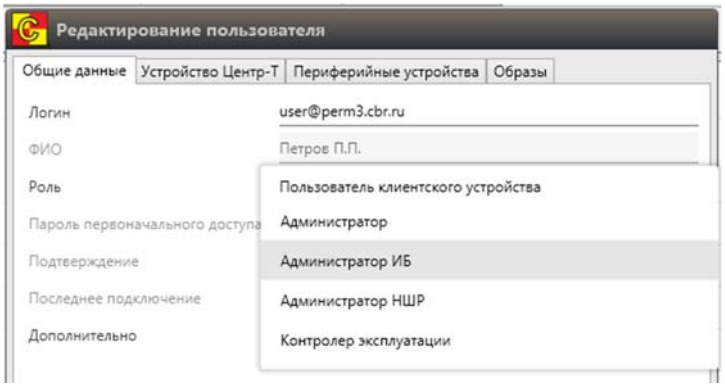


Рисунок 66 – Назначение новой роли учетной записи

После смены роли пользователю, которому назначается роль администратора удаленного управления, нужно обязательно задать пароль.

Для учетной записи администратора удаленного управления, которой назначается другая административная роль, после смены роли в

окне настроек учетной записи по умолчанию указаны пароль и идентификатор, соответствующие учетной записи до выполнения процедуры. Идентификатор может быть изменен только от имени самой редактируемой учетной записи.

ВНИМАНИЕ! Администратор БИ не может менять роль учетной записи, от имени которой в текущий момент выполняется смена роли.

Для учетной записи пользователя клиентского устройства необходимо задать параметры клиентского устройства (см.5.8) и терминала пользователя (см. 5.9), назначить образ ПО ТС и шаблон настроек образа (см. 5.10). Выполнение указанных настроек не требуется, если назначение роли пользователя выполняется для последующего удаления учетной записи.

ВНИМАНИЕ! Все параметры, установленные учетной записи до смены роли, сбрасываются.

Строка «Блокировка пользователя» позволяет заблокировать работу пользователя. Если до блокировки статус пользователя был рабочим («Работает»), то при выставлении галочки в этой строке (и сохранении изменений) статус изменится на «Заблокирован/Работает» (рисунок 67). При выключении терминала пользователя установится статус «Заблокирован», и при последующем его включении будет выдана ошибка синхронизации с сервером.

test1@misha	qwyse8gb	Пользователь клиентского устрои	36000795	Заблокирован/Работает	10.07.2023 17:15:20	4437
test134@misha	centertrust	Пользователь клиентского устрои	36001149	Заблокирован	10.07.2023 11:57:59	5866

Рисунок 67 – Изменение статуса пользователя при его блокировке

В поле «Режим оповещения пользователя» (рисунок 65) есть возможность настройки функции отправки информационного сообщения пользователю клиентского устройства. Сообщение может отправляться при запуске клиентского устройства - однократно или при каждом старте (при выборе соответствующей опции в строке «Оповещать пользователя при старте»), а также в произвольный момент времени (при отметке строки «Выслать оповещение сейчас»). Текст информационного сообщения вводится в строке «Текст оповещения:».

Если клиентское устройство пользователя, которому отправлено оповещение в текущий момент времени («сейчас»), выключено (недоступно), появляется сообщение «Пользователь не в сети», а в журнале регистрации фиксируется ошибка отправки сообщения. В противном случае оповещение появляется на мониторе пользователя поверх всех открытых подключений через несколько секунд (в зависимости от загруженности сети) после отправки сообщения Администратором ИБ.

При отметке нескольких пользователей на вкладке «Пользователи» и выборе команды контекстного меню «Отправить оповещение…» появляется окно ввода информационного сообщения для массовой рассылки (рисунок 68).

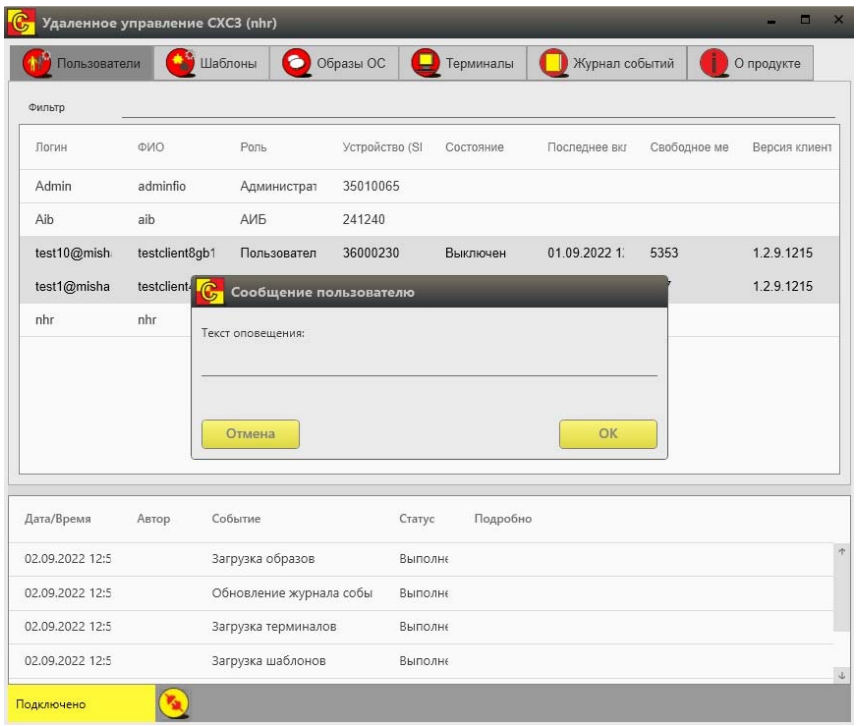


Рисунок 68 – Окно ввода текста оповещения для массовой рассылки

При данном способе отправки сообщений в случае задания режима оповещения при старте у выбранных пользователей текст, показываемый при запуске, не будет изменен.

Сообщение от Администратора БИ, отображаемое пользователю при старте клиентского устройства, имеет вид, показанный на рисунке 69 .

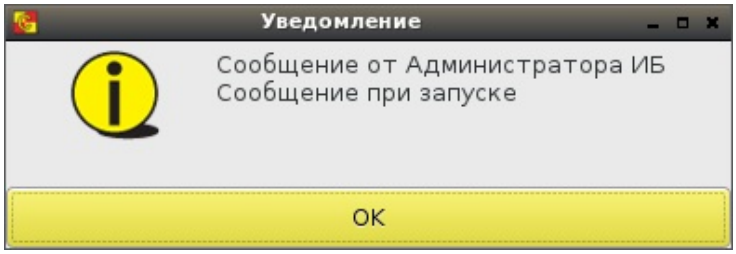


Рисунок 69 – Вид отображаемого пользователю сообщения при запуске клиентского устройства

Вид отображаемого пользователю сообщения, отправленного в режиме «Выслать оповещение сейчас» или при массовой рассылке нескольким пользователям, показан на рисунке 70.

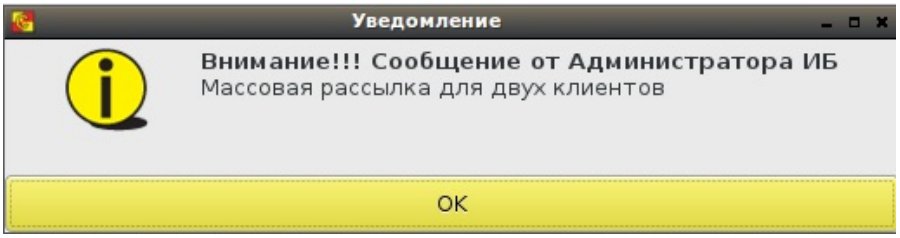


Рисунок 70 - Вид отображаемого пользователю сообщения при массовой рассылке или отправленного в произвольный момент времени

Сохранение изменений в окне редактирования настроек учетной записи пользователя производится по кнопке <Сохранить>.

5.8. Назначение пользователю клиентского устройства

После того как Администратор СХСЗ создал учетные записи пользователей, Администратор БИ, получив журнал, в котором серийные номера клиентских устройств соотнесены ФИО пользователей, должен выполнить процедуру назначения клиентских устройств пользователям.

Для назначения клиентского устройства учетной записи пользователя необходимо перейти на вкладку «Пользователи» (рисунок 63), выбрать нужную учетную запись пользователя и нажать клавишу «Enter» или вызвать команду «Редактировать» из контекстного меню. При этом появляется окно с настройками пользователя, доступными администраторам удаленного управления СХСЗ (рисунок 71).

В поле «Серийный номер» на вкладке «Устройство Центр-Т» следует ввести вручную серийный номер клиентского устройства (специального носителя ПО ПАК Центр-Т). После начала эксплуатации Комплекса на этой вкладке также отображаются тип подключенного носителя ПО, объем свободной памяти, интервал подключения к сервису RMQ, настройки кэширования и IP-адрес терминала, загруженного с клиентского устройства пользователя (IP-адрес клиентского устройства).

Помимо серийного номера Администратор БИ может настроить удаление событий безопасности на клиентском устройстве. Выбор параметра «Удалять события после передачи их на сервер» позволяет использовать функцию очищения журнала регистрации событий клиентского устройства после передачи записей журнала на СХСЗ (процедура осуществляется в начале работы с клиентским устройством). Данная настройка может быть установлена сразу для нескольких учетных записей.

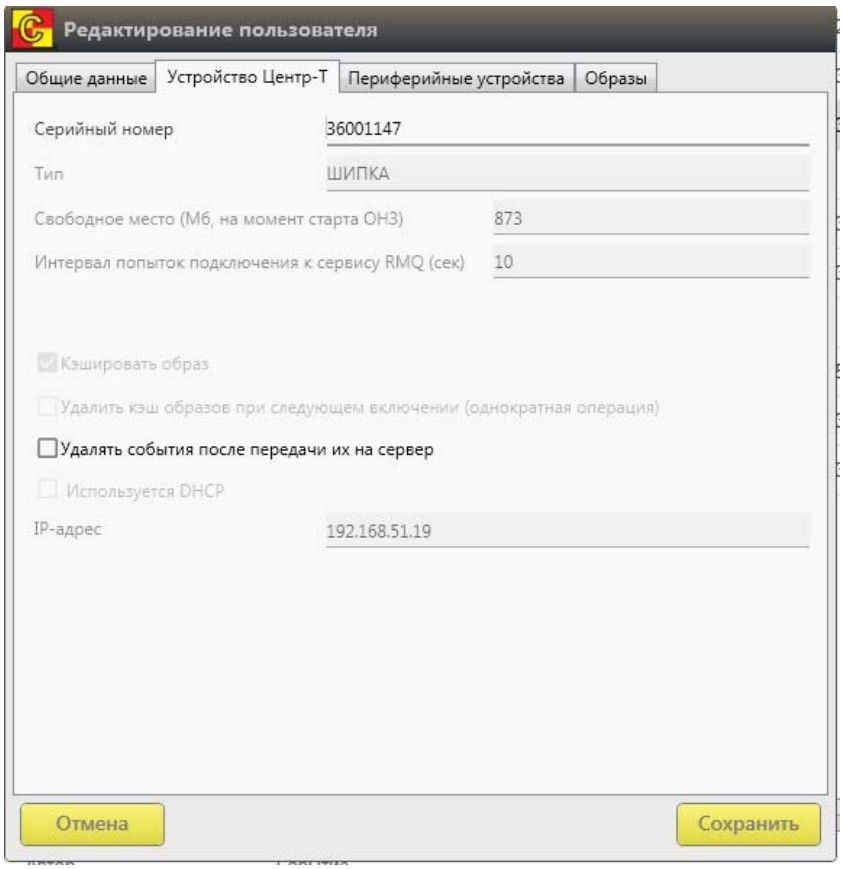


Рисунок 71 – Вкладка «Устройство Центр-Т» окна «Редактирование пользователя»

Сохранение изменений осуществляется по кнопке <Сохранить>.

После назначения клиентских устройств Администратору БИ следует назначить пользователям образы ПО ТС, шаблоны настроек образов (см. 5.10) и справочники сертификатов.

ВНИМАНИЕ! Следует помнить, что запуск большого количества терминальных клиентов одновременно даст нагрузку на сеть (не на носитель ПО СХСЗ).

Для уменьшения нагрузки сети рекомендуется использовать функцию кэширования образа.

5.9. Просмотр информации о терминалах пользователей

Информация о терминалах, на которых пользователи производили загрузку ПО Клиента с назначенных им специальных носителей, хранится в базе данных СХСЗ и доступна к просмотру на вкладке «Терминалы» (рисунок 72).

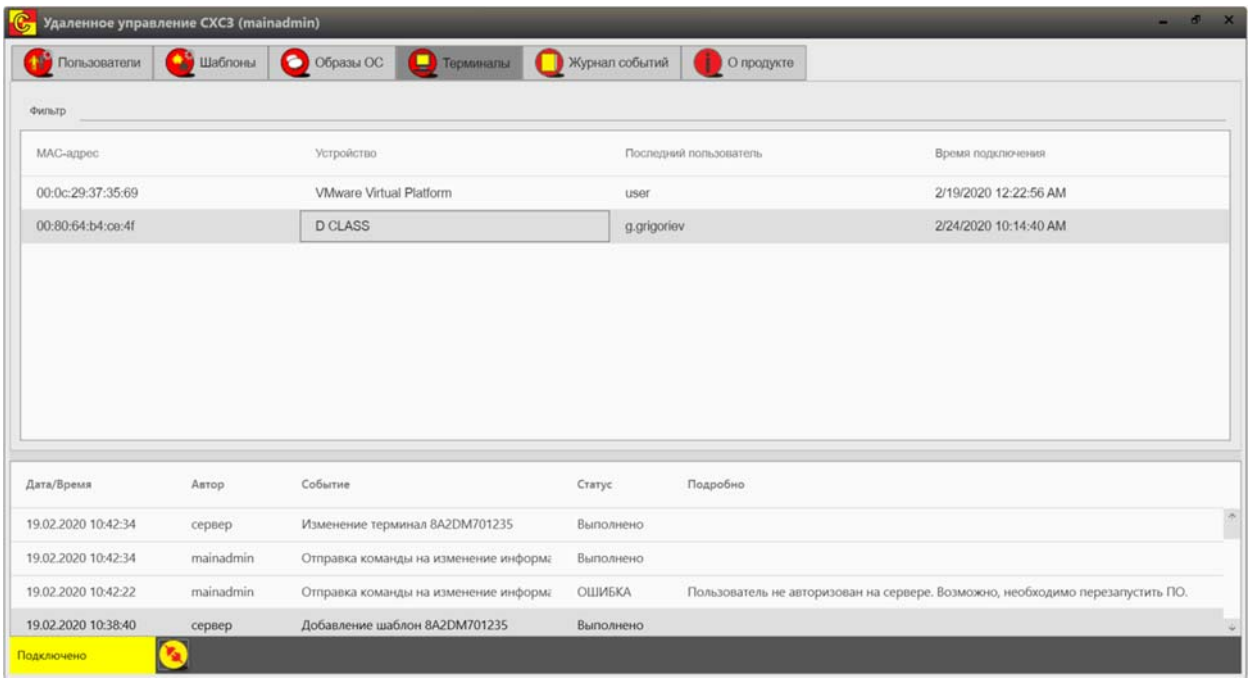


Рисунок 72 – Вкладка «Терминалы»

Список используемых терминалов ведется по МАС-адресу. Более подробную информацию по конкретному терминалу можно посмотреть при вызове правой кнопкой мыши контекстного меню и выборе команды <Подробнее> (рисунок 73).

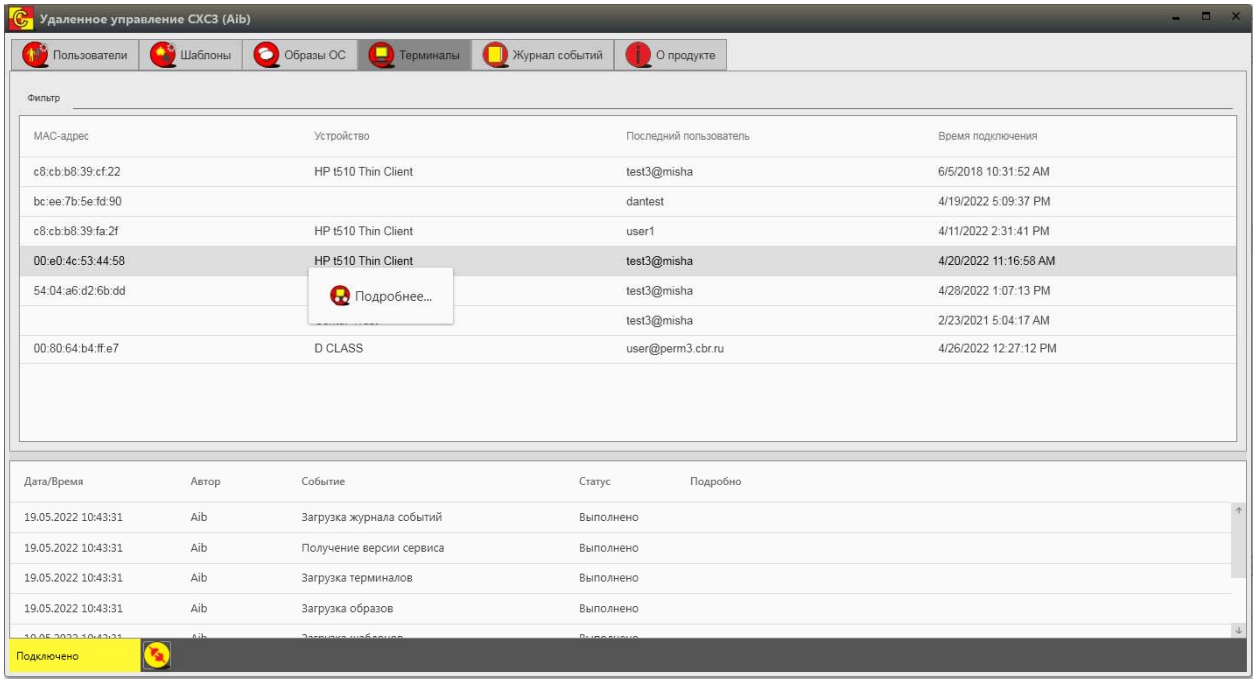


Рисунок 73 – Контекстное меню вкладки «Терминалы»

В появившемся окне «Информация о терминале» (рисунок 74) можно просмотреть основные данные терминала.

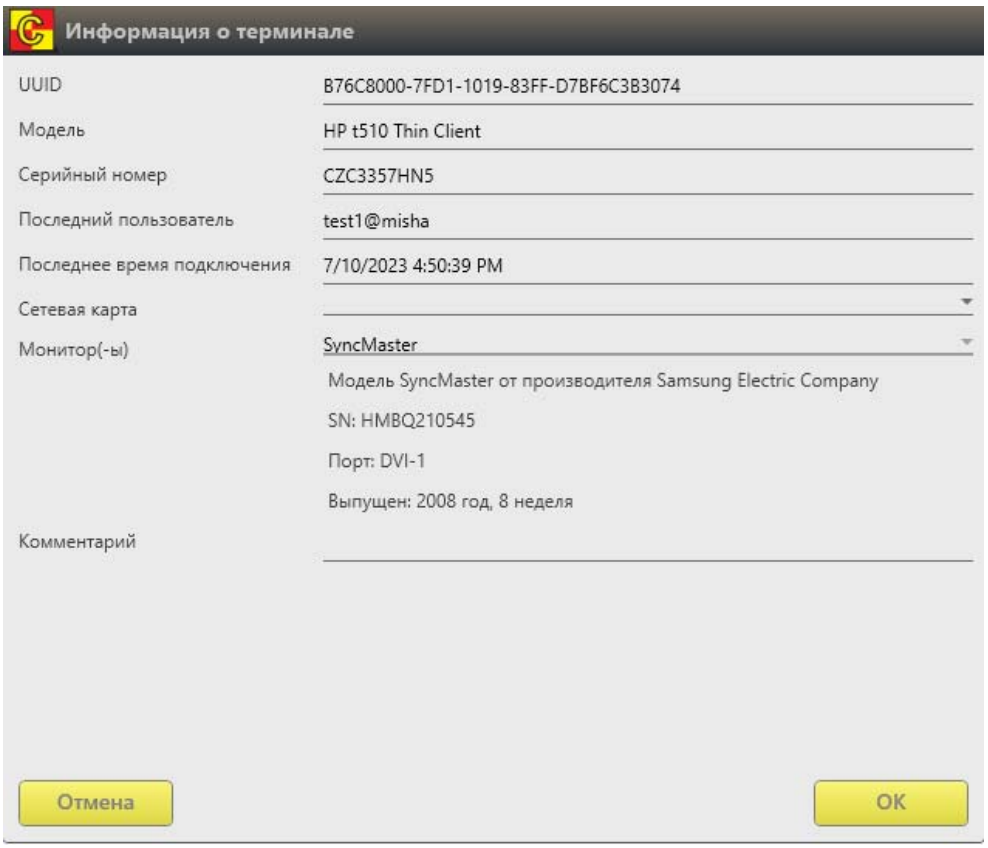


Рисунок 74 – Окно «Информация о терминале»

Обратите внимание, что информация об используемом мониторе, собираемая с клиентского рабочего места, может отличаться для одних и тех же моделей терминала и монитора в зависимости от используемого интерфейса подключения.

5.10. Назначение пользователю образов и шаблонов настроек ПО ТС

Назначение пользователю образа ПО ТС производится на вкладке «Пользователи» (рисунок 63). Необходимо выбрать нужную учетную запись пользователя (или несколько), вызвать меню нажатием правой кнопки мыши и в появившемся окне выбрать пункт «Редактировать». После этого появляется окно с настройками пользователя, доступными Администратору БИ. В появившемся окне следует перейти на вкладку «Образы» (рисунок 75).

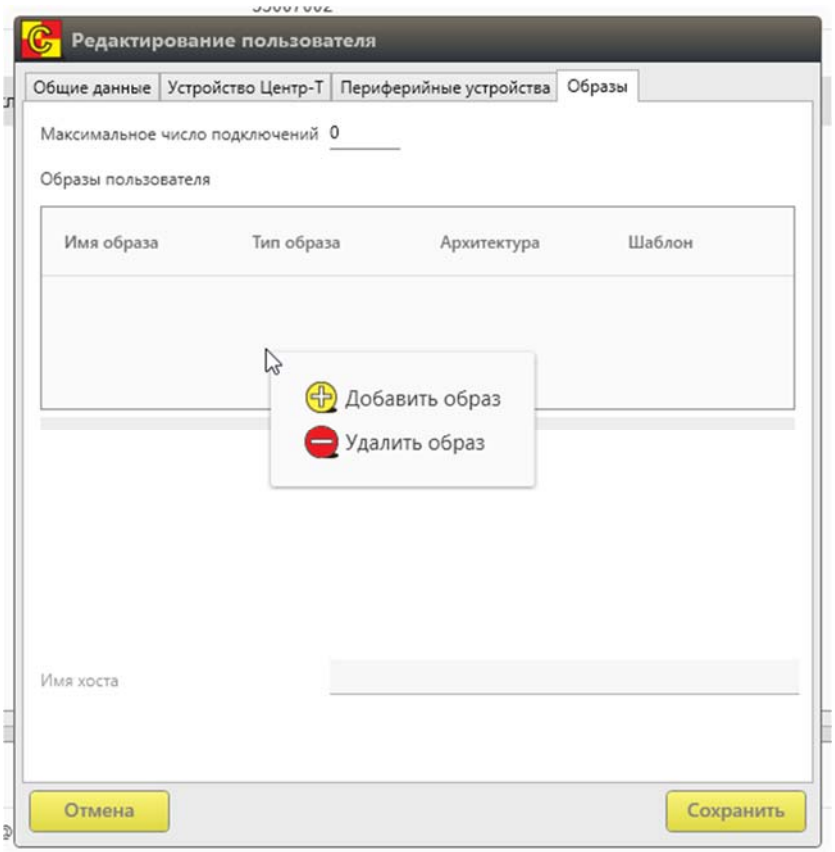


Рисунок 75 – Вкладка «Образы»

Каждому пользователю могут быть назначены одна или несколько пар Образ-Шаблон. Каждая такая пара определяет, с каким терминальным сервером Citrix (задается в шаблоне, см. п.5.5) может работать пользователь, а также как будет осуществляться подключение к этому терминальному серверу (определяется назначенным образом, см. п.5.6).

При назначении пары Образ-Шаблон необходимо учитывать архитектуру терминальных станций, на которых работает пользователь, - архитектура назначаемого образа должна ей соответствовать. В случае если Пользователь работает как на терминальных станциях с архитектурой x86-64, так и на Защищенном терминале Центр-TrusT, необходимо назначать для него Образы обеих архитектур. Если не будет назначено ни одного подходящего по архитектуре образа, при попытке подключения к СХС3 такой Пользователь получит соответствующую ошибку. Если же среди назначенных найдутся подходящие по архитектуре образы, подключения к терминальному серверу будут открыты в соответствии с ними (подробнее см. Руководство по эксплуатации клиентских устройств, раздел 5.3)[8].

Для назначения пары Образ-Шаблон необходимо нажать правой кнопкой мыши на область таблицы «Образы» и выбрать пункт меню «Добавить образ». В появившемся окне «Добавление образа»

[8] В случае версии ПО Клиента ниже 1.2.8 и назначении Пользователю хотя бы одного образа неподходящей архитектуры (ARM64) произойдёт ошибка подключения. Подробнее о совместимости ПАК «Центр-Т» разных версий – в Приложении 7.

(рисунок 76) следует выбрать из выпадающих списков имена образа и шаблона, после чего нажать кнопку «Установить». Заданная пара Образ-Шаблон появится в таблице «Образы» (рисунок 77).

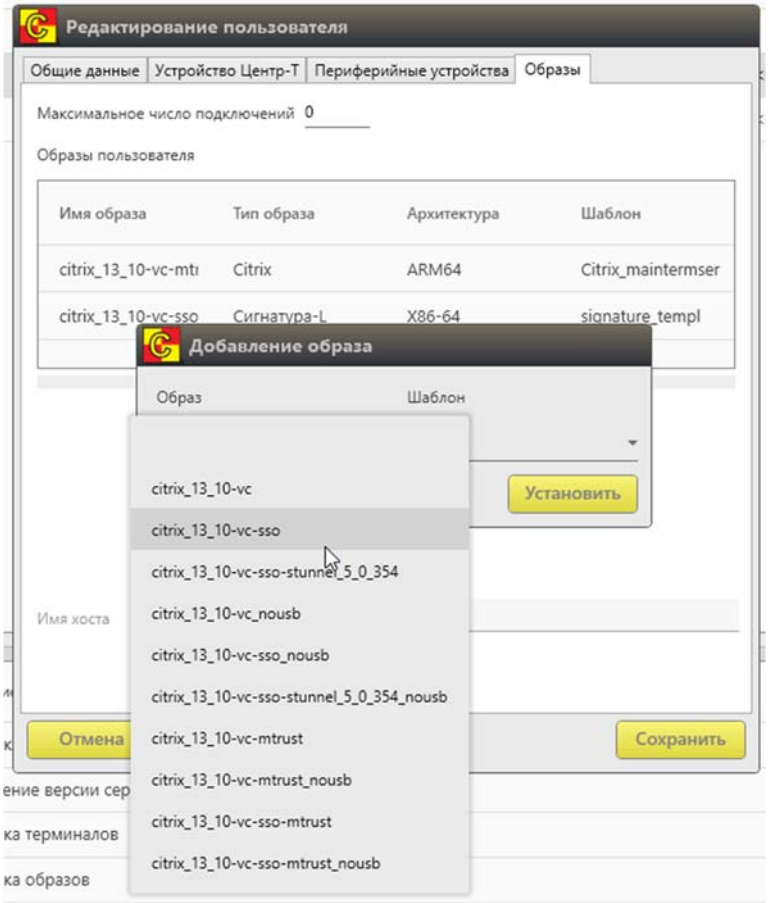


Рисунок 76 - Окно добавления пары Образ-Шаблон

Обратите внимание, что в каждой паре Образ-Шаблон тип шаблона обязательно должен соответствовать типу образа.

Если пользователю назначена пара Образ-Шаблон, поддерживающий работу со СКАД Сигнатура-L (тип образа «Сигнатура-L»), необходимо назначить также справочники сертификатов или сертификат корневого Центра Сертификации для каждой такой пары.

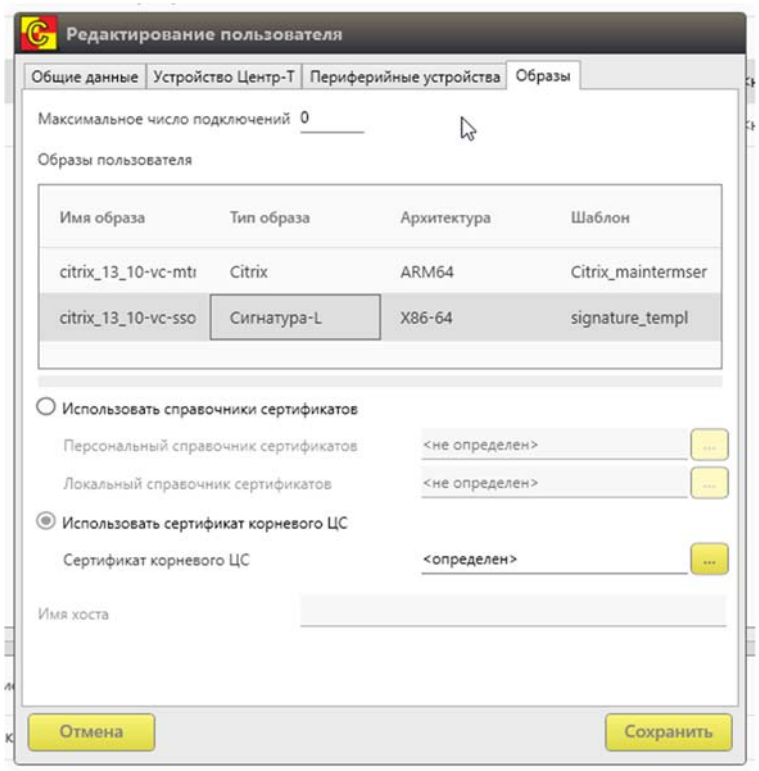


Рисунок 77 - Таблица «Образы»

Процедура назначения справочников сертификатов выполняется в окне настроек пользователя, вкладка «Образы», при нажатии на пару Образ-Шаблон типа «Signature» (рисунок 77) и включает в себя:

- выбор пункта «Использовать справочники сертификатов»;
  - назначение персонального справочника сертификатов (local.pse);
  - назначение локального справочника сертификатов (local.gdbm)
- выбор пункта «Использовать сертификат коневого ЦС»
  - назначение сертификата корневого Центра Сертификации (PSEStore).

Для назначения справочника/сертификата необходимо нажать кнопку ... и указать требуемый файл.

ВНИМАНИЕ! Для корректной работы образа СКАД Сигнатура-L необходимо выполнить ряд дополнительных действий:

1) справочники для ПО СКАД Сигнатура-L необходимо экспортировать в платформонезависимом формате;

2) полученные справочники предварительно импортировать на любом Linux СВТ с установленным СКАД Сигнатура-L (при импорте справочники конвертируются в необходимый формат);

3) полученные после импорта на этапе 2 справочники использовать для работы в ПАК «Центр-Т».

Также для пользователя Администратор БИ определяет максимальное число одновременных подключений к терминальным серверам, которые могут быть открыты на Клиентском устройстве. Для задания указанного параметра Администратор БИ должен указать численное значение в поле «Максимальное число подключений» (разрешен ввод только неотрицательных целых чисел). Значение «0», заданное по умолчанию, обозначает, что число одновременных подключений не ограничено. Обратите внимание, что при работе пользователя клиентского устройства на Центр-TrusT максимальное число подключений не должно быть более двух.

Сохранение изменений осуществляется по кнопке <Сохранить>.

В случае назначения сертификата корневого Центра Сертификации при первом старте терминальной сессии пользователя произойдет генерация персонального и локального справочников сертификатов пользователя и их передача на Сервер. В дальнейшем при работе Клиента в терминальной сессии будут использоваться сгенерированные персональный и локальный справочники сертификатов.

ВНИМАНИЕ! При выборе образов с возможностью проброса USB-устройств в терминальную сессию потребуется дополнительная настройка Citrix на терминальном сервере, так как по умолчанию перенаправление USB-устройств в настройках Citrix не включено. Если в настройках проброс будет разрешен (включен), USB--устройство будет проброшено в терминальную сессию. Соответствующие настройки Citrix описаны по ссылке https://support.citrix.com/article/CTX137939

5.11. Экспорт списка пользователей в файл .csv

Экспорт списка пользователей Администратор БИ выполняет аналогично Администратору СХСЗ (раздел 4.5.4).

5.12. Просмотр событий безопасности

Администратор БИ может просматривать события безопасности:

- собственной сессии;
- сессии администраторов удаленного управления СХСЗ;
- сессий пользователей клиентских устройств.

Указанные события фиксируются в общем журнале и отображаются на вкладке «Журнал событий» (рисунок 53).

События текущей сессии отображаются в нижней части окна вкладки «Журнал событий».

Общий журнал хранится в БД (внутренней или внешней, в зависимости от настроек СХСЗ) и не перезаписывается при выключении или перезагрузке как СХСЗ, так и внешней СУБД.

Для поиска нужной информации в событиях можно использовать функцию фильтра, доступную в верхней части окна. Применение фильтра происходит при нажатии на клавишу «Enter», поиск осуществляется с учетом регистра. Для удаления фильтра необходимо удалить искомый текст и вновь нажать клавишу «Enter».

Также есть возможность просмотра события за определенный период. Для использования этой функции нужно выбрать период отображаемых записей в правой части окна и нажать кнопку <Применить>. Доступны следующие варианты:

- за сегодня (по умолчанию);
- за предыдущий день;
- за неделю;
- за месяц;
- за указанный (произвольный) период;
- за все время.

ВНИМАНИЕ! События, отображаемые в журнале, указаны по текущему времени на рабочем месте Администратора БИ, на котором установлена утилита удаленного управления, при этом фильтры по временному периоду работают со временем событий в UTC.

При нажатии кнопки <Экспорт> доступна функция экспорта журнала событий. Экспорт записей производится в соответствии с заданным фильтром по времени в текстовом формате в файл с расширением .txt.

5.13. Восстановление сессии пользователя

В статусной строке главного окна программы удаленного управления СХСЗ отображается индикатор наличия связи с сервером RMQ – желтая надпись «Подключено» (рисунок 78). Рядом с ней располагается кнопка для проверки подключения.

Рисунок 78 – Статус «Подключено»

В случае если в процессе работы происходит потеря связи с сервером RMQ, цвет индикатора меняется на серый, а сообщение – на «Связь потеряна» (рисунок 79).

Рисунок 79 – Статус «Связь потеряна»

Если связь будет восстановлена, то программа автоматически возобновит подключение. Пользователь может проверить наличие подключения вручную, кликнув по кнопке <Проверить подключение>.

В случае потери связи пользователь может просматривать данные, но не может выполнять никаких операций добавления, удаления или редактирования.

5.14. Просмотр информации о продукте и статусе лицензии СХСЗ

Администратор ИБ может просматривать информацию о продукте, а также о статусе лицензии на СХСЗ. Подробнее – раздел 4.11.

5.15. Завершение работы ПО управления

Для завершения работы Администратор ИБ должен нажать кнопку  в ПО управления СХСЗ и завершить работу с ПО удаленного доступа к СХСЗ.

6. Состав работ Администратора НШР

6.1. Общие сведения

По умолчанию в БД ПАК «Центр-Т» нет учетной записи с ролью Администратора НШР; при необходимости она должна быть создана Администратором в процессе эксплуатации Комплекса.

После того как Администратор БИ назначит новой учетной записи роль и задаст пароль, Администратор НШР сможет приступить к выполнению своих функциональных обязанностей.

В рамках своих обязанностей Администратор НШР имеет права на выполнение любых настроек ПО управления СХСЗ.

6.2. Установка ПО для удаленного доступа к СХСЗ

Установка ПО для удаленного доступа к СХСЗ выполняется Администратором НШР на собственном АРМ так же, как и для Администратора СХСЗ (см. 4.2).

6.3. Получение доступа к ПО управления СХСЗ

Процедура получения доступа Администратора НШР к ПО управления СХСЗ выполняется в целом так же, как и аналогичная процедура для Администратора (см. 4.3). Отличие состоит в том, что Администратор НШР не имеет параметров идентификации по умолчанию. Предварительно Администратором СХСЗ должна быть создана учетная запись, а Администратором БИ – назначение этой учетной записи роли Администратора НШР и пароля первоначального доступа. После этого логин и пароль первоначального доступа должны быть переданы лицу, выполняющему роль Администратора НШР, и использованы для первого входа.

При первом входе в ПО управления СХСЗ выполняется принудительное изменение пароля и назначение собственного идентификатора. Порядок выполнения процедуры назначения устройства и нового пароля указан в пункте 6.4. В дальнейшем смена пароля/идентификатора может быть произведена в любое время.

Если идентификация Администратора НШР выполнена успешно, появляется главное окно ПО управления СХСЗ с доступными Администратору НШР настройками.

Учетная запись, от имени которой работает Администратор НШР, указана в строке с названием утилиты.

6.4. Изменение параметров идентификации Администратора НШР

Для идентификации Администратор НШР использует пароль и отчуждаемое аппаратное устройство.

Для изменения параметров идентификации Администратору НШР необходимо перейти на вкладку «Пользователи» в главном окне ПО управления СХСЗ и выбрать собственную учетную запись. Далее правой кнопкой мыши следует вызвать окно доступных действий и выбрать пункт «Редактировать». При этом появляется окно настроек учетной записи Администратора НШР (рисунок 80). В появившемся окне нужно ввести старый пароль и новый пароль Администратора НШР с подтверждением, если требуется сменить пароль; если необходимо назначить/изменить идентификатор Администратора НШР, то следует подключить и выбрать в списке новое устройство.

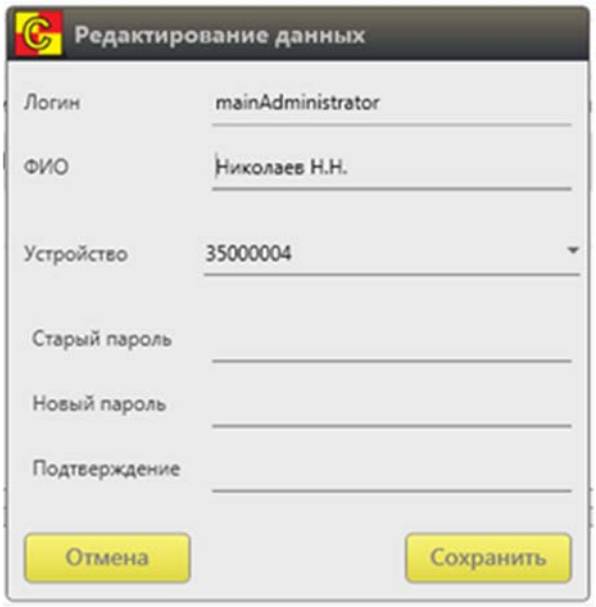


Рисунок 80 - Окно настроек учетной записи Администратора НШР

Сохранение параметров идентификации Администратора НШР выполняется по кнопке <Сохранить>. После выполнения необходимых настроек следует перезапустить утилиту.

6.5. Управление учетными записями

6.5.1. Создание учетных записей

Администратор НШР имеет право создавать новые учетные записи.

Для создания новой учетной записи необходимо на вкладке «Пользователи» нажать правой кнопкой мыши в любом месте таблицы учетных записей и выбрать пункт «Создать» в меню доступных действий. При этом появляется окно создания учетной записи пользователя (рисунок 37).

Процедура создания учетных записей выполняется аналогично их созданию от имени Администратора СХСЗ (раздел 4.5.1).

6.5.2. Редактирование учетных записей

Для изменения параметров учетной записи необходимо на вкладке «Пользователи» выбрать нужную запись и вызвать контекстное меню нажатием правой кнопки мыши. В появившемся окне следует выбрать пункт «Редактировать». При этом на экране появляется окно редактирования учетной записи пользователя.

В случае редактирования учетных записей администраторов удаленного управления СХСЗ Администратору НШР доступна смена логина, ФИО и роли, а также задание поля «Дополнительно».

В случае редактирования учетных записей пользователей клиентского устройства Администратору НШР доступны:

- смена ФИО и логина;
- смена роли;
- задание поля «Дополнительно»;
- назначение пользователю клиентского устройства (задание серийного номера идентификатора);
- настройка разрешения экрана (возможна после первого подключения пользователя к СХСЗ);
- настройка параметров кэширования образа ПО ТС на устройстве пользователя;
- настройка параметра удаления событий безопасности на клиентском устройстве;
- просмотр следующих параметров: дата и время последнего подключения, объем свободной памяти момент старта ОНЗ, настройки сети (IP-адрес клиентского устройства), интервал подключения к сервисам RMQ;
- просмотр информации об используемом Клиентами оборудовании;
- назначение образов и шаблонов настроек ПО ТС.

Все настройки выполняются аналогично их заданию Администратором или Администратором БИ (разделы 4.5, 5.7-5.11).

При редактировании собственной учетной записи Администратору СХСЗ помимо смены логина и ФИО доступны также изменения пароля и идентификатора.

6.5.3. Удаление учетных записей

Удаление учетных записей Администратор НШР выполняет аналогично Администратору СХСЗ (раздел 4.5.3).

6.5.4. Экспорт пользователей в файл .csv

Экспорт списка пользователей Администратор НШР выполняет аналогично Администратору СХСЗ (раздел 4.5.4).

6.6. Задание параметров терминала пользователя

Администратор НШР может просматривать параметры терминала пользователя. Подробнее о просмотре этих параметров см. п. 5.9.

6.7. Просмотр информации о терминалах пользователей

Администратор НШР может просматривать информацию о терминалах пользователей после их загрузки со специального носителя, назначенного Администратором БИ пользователю. Подробнее о просмотре информации об оборудовании пользователей см. п.5.9.

6.8. Просмотр образов ПО ТС

Текущие образы ПО ТС отображены на вкладке «Образы ОС». Все доступные на данный момент образы подробно описаны в п.5.5.

6.9. Управление шаблонами настроек образов ПО ТС

6.9.1. Создание шаблона настроек образа

Администратор НШР имеет право на создание шаблонов настроек образа. Действие выполняется аналогично действиям Администратора СХСЗ (раздел 4.7.1).

6.9.2. Редактирование шаблона настроек образа

Администратор НШР имеет право на редактирование шаблонов настроек образа. Действие выполняется аналогично действиям Администратора СХСЗ (раздел 4.7.2).

6.9.3. Удаление шаблона настроек образа

Администратор НШР имеет право на удаление шаблонов настроек образа. Действие выполняется аналогично действиям Администратора СХСЗ (раздел 4.7.3).

6.10. Просмотр событий безопасности

Администратор НШР может просматривать события безопасности:

- собственной сессии;
- сессии администраторов удаленного управления СХСЗ;
- сессий пользователей клиентских устройств.

Указанные события фиксируются в общем журнале и отображаются на вкладке «Журнал событий» (рисунок 53).

События текущей сессии отображаются в нижней части окна вкладки «Журнал событий».

Общий журнал хранится в БД (внутренней или внешней, в зависимости от настроек СХСЗ) и не перезаписывается при выключении или перезагрузке как СХСЗ, так и внешней СУБД.

Для поиска нужной информации в событиях можно использовать функцию фильтра, доступную в верхней части окна. Применение фильтра происходит по нажатию на клавишу «Enter», поиск осуществляется с учетом регистра. Для удаления фильтра необходимо удалить искомый текст и вновь нажать клавишу «Enter».

Также есть возможность просмотра события за определенный период. Для использования этой функции нужно выбрать период отображаемых записей в правой части окна и нажать кнопку <Применить>. Доступны следующие варианты:

- за сегодня (по умолчанию);
- за предыдущий день;
- за неделю;
- за месяц;
- за указанный (произвольный) период.

ВНИМАНИЕ! События, отображаемые в журнале, указаны по текущему времени на рабочем месте Администратора НШР, на котором установлена утилита удаленного управления, при этом фильтры по временному периоду работают со временем событий в UTC.

При нажатии кнопки <Экспорт> доступна функция экспорта журнала событий. Экспорт записей производится в соответствии с заданным фильтром по времени в текстовом формате в файл с расширением .txt.

6.11. Восстановление сессии пользователя

В статусной строке главного окна программы удаленного управления СХСЗ отображается индикатор наличия связи с сервером RMQ – желтая надпись «Подключено». Рядом с ней располагается кнопка для проверки подключения (рисунок 78).

В случае если в процессе работы происходит потеря связи с сервером RMQ, цвет индикатора меняется на серый, а сообщение – на «Связь потеряна» (рисунок 79).

Если связь будет восстановлена, то программа автоматически возобновит подключение. Пользователь может проверить наличие подключения вручную, кликнув по кнопке <Проверить подключение>.

В случае потери связи пользователь может просматривать данные, но не может выполнять операции добавления, удаления или редактирования.

6.12. Просмотр информации о продукте и статусе лицензии СХСЗ

Администратор НШР может просматривать информацию о продукте, а также о статусе лицензии на СХСЗ. Подробнее – раздел 4.11.

6.13. Завершение работы ПО управления

Для завершения работы Администратор НШР должен нажать кнопку  в ПО управления СХСЗ и завершить работу с ПО удаленного доступа к СХСЗ.

7. Состав работ Контролера эксплуатации

7.1. Общие сведения

По умолчанию в БД ПАК «Центр-Т» нет учетной записи с ролью Контролера эксплуатации; при необходимости она должна быть создана Администратором в процессе эксплуатации Комплекса.

После того как Администратор БИ назначит новой учетной записи роль и задаст пароль, Контролер сможет приступить к выполнению своих функциональных обязанностей.

В рамках своих обязанностей Контролер может просматривать все настройки, заданные другими администраторами удаленного управления СХСЗ, но не имеет прав на выполнение настроек СХСЗ (кроме задания собственных параметров идентификации).

7.2. Установка ПО для удаленного доступа к СХСЗ

Установка ПО для удаленного доступа к СХСЗ выполняется Контролером на собственном АРМ так же, как и для Администратора СХСЗ (см. 4.2).

7.3. Получение доступа к ПО управления СХСЗ

Процедура получения доступа Контролера к ПО управления СХСЗ выполняется в целом так же, как и аналогичная процедура для Администратора (см. 4.3). Отличие состоит в том, что Контролер не имеет параметров идентификации по умолчанию. Предварительно Контролером должна быть создана учетная запись, а Администратором БИ – назначение этой учетной записи роли Контролера и пароля первоначального доступа. После этого логин и пароль первоначального доступа должны быть переданы лицу, выполняющему роль Контролера, и использованы для первого входа.

При первом входе в ПО управления СХСЗ выполняется принудительное изменение пароля и назначение собственного идентификатора. Порядок выполнения процедуры назначения устройства и нового пароля указан в пункте 7.4. В дальнейшем смена пароля/идентификатора может быть произведена в любое время.

Если идентификация Контролера выполнена успешно, появляется главное окно ПО управления СХСЗ с доступными Контролеру настройками.

Учетная запись, от имени которой работает Контролер, указана в строке с названием утилиты.

7.4. Изменение параметров идентификации Контролера

Для идентификации Контролер использует пароль и отчуждаемое аппаратное устройство.

Для изменения параметров идентификации Контролеру необходимо перейти на вкладку «Пользователи» в главном окне ПО управления СХСЗ и выбрать собственную учетную запись двойным щелчком левой клавиши мыши. При этом появляется окно настроек учетной записи Контролера (рисунок 81). В появившемся окне нужно ввести старый пароль и новый пароль Контролера с подтверждением, если требуется сменить пароль; если необходимо назначить/изменить идентификатор, следует подключить и выбрать в списке новое устройство.

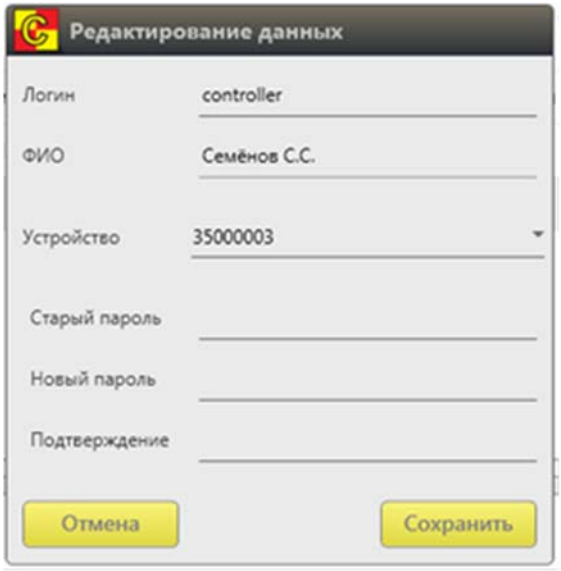


Рисунок 81 - Окно настроек учетной записи Контролера

Сохранение параметров идентификации Контролера выполняется по кнопке <Сохранить>. После выполнения необходимых настроек следует перезапустить утилиту.

7.5. Просмотр учетных записей пользователей

Контролер имеет право на просмотр всех настроек, заданных учетным записям.

Для просмотра параметров учетной записи необходимо на вкладке «Пользователи» выбрать нужную запись и вызвать контекстное меню нажатием правой кнопки мыши. В появившемся окне следует выбрать пункт «Просмотр». При этом на экране появляется окно просмотра учетной записи пользователя (рисунок 82).

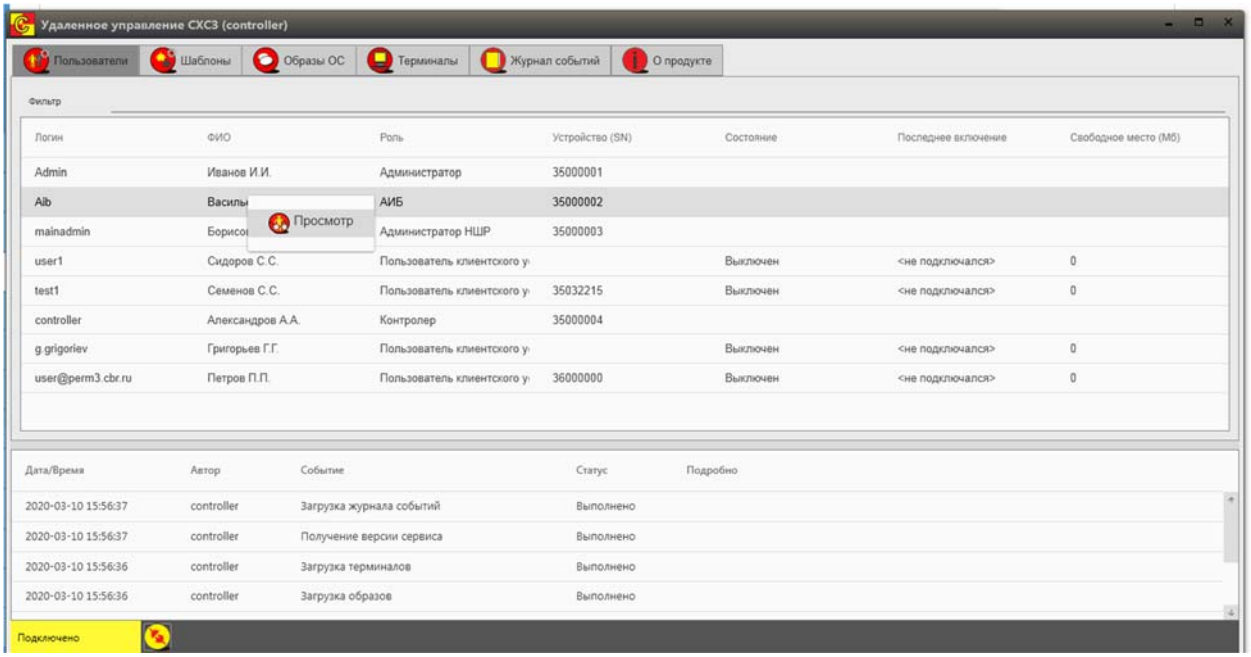


Рисунок 82 - Окно просмотра учетной записи пользователя

В случае просмотра учетных записей администраторов удаленного управления СХСЗ Контролеру доступна информация о логине, ФИО и роли, а также значение поля «Дополнительно» (рисунок 83).

Рисунок 83 - Окно просмотра учетных записей администраторов удаленного управления СХСЗ

В случае просмотра учетных записей пользователей клиентского устройства Контролеру доступны:

– ФИО и логин;

- роль;
- поле «Дополнительно» (рисунок 84);
- назначенное пользователю клиентское устройство (серийный номер идентификатора), в том числе его тип;
- настройка разрешения экрана (возможна после осуществления первого подключения пользователя к СХСЗ);
- настройка параметров кэширования образа ПО ТС на устройстве пользователя;
- настройка параметра удаления событий безопасности на клиентском устройстве;
- дата и время последнего подключения;
- объем свободной памяти на момент старта ОНЗ, настройки сети (IP-адрес клиентского устройства), интервал подключения к сервисам RMQ (рисунок 85);
- заданный образ и шаблоны настроек ПО ТС (рисунок 86).

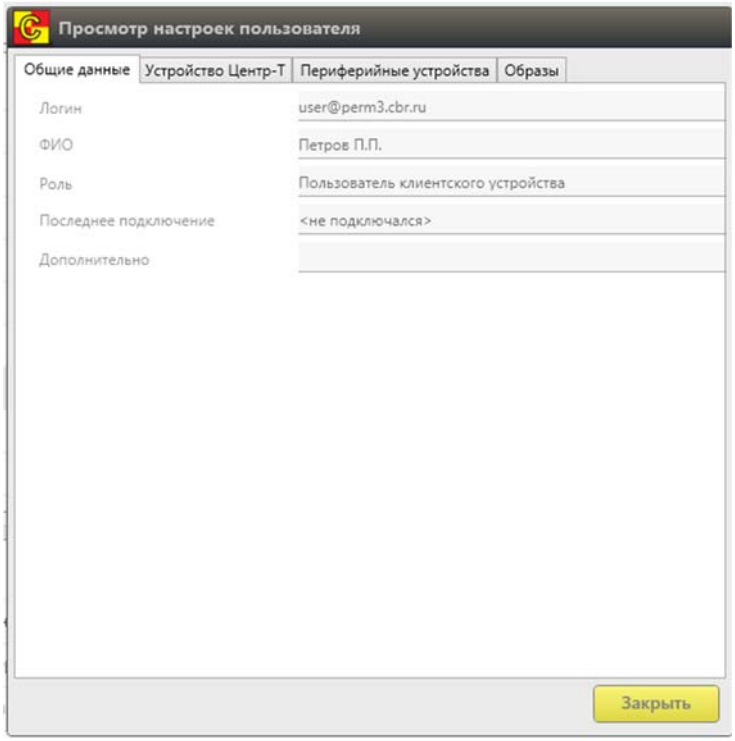


Рисунок 84 - Окно просмотра учетных записей пользователей клиентского устройства. Общие данные

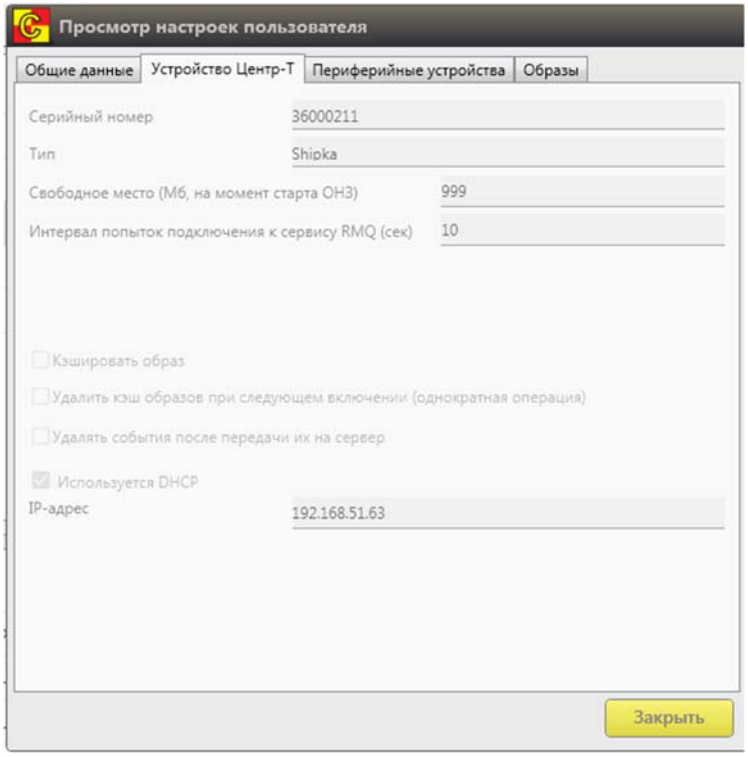


Рисунок 85 - Окно просмотра учетных записей пользователей клиентского устройства. Устройство Центр-Т

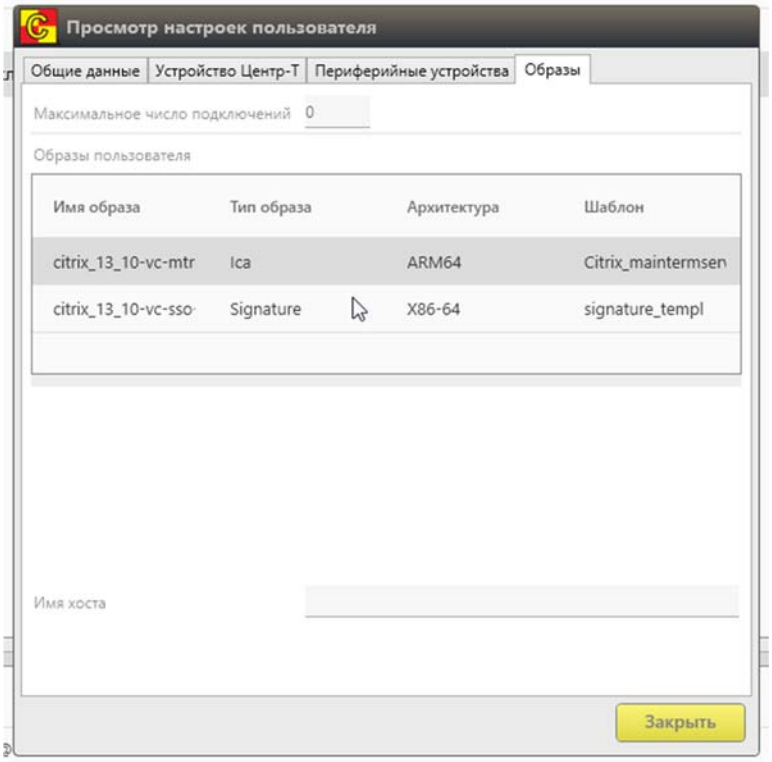


Рисунок 86 - Окно просмотра учетных записей пользователей клиентского устройства. Образы

7.6. Экспорт пользователей в файл .csv

Экспорт списка пользователей Контролер выполняет аналогично Администратору СХСЗ (раздел 4.5.4).

7.7. Просмотр информации о терминалах пользователей

Контролер может просматривать информацию о терминалах пользователей после их загрузки со специального носителя, назначенного Администратором БИ пользователю. Подробнее о просмотре информации об оборудовании пользователей см. п.5.9.

7.8. Просмотр образов ПО ТС

Текущие образы ПО ТС отображены на вкладке «Образы ОС». Все доступные на данный момент образы подробно описаны в п.5.5.

7.9. Просмотр шаблонов настроек образов ПО ТС

Контролер имеет право на просмотр всех шаблонов настроек образов ПО ТС.

Для просмотра параметров шаблонов настроек образов ПО ТС необходимо на вкладке «Шаблоны» выбрать нужную запись и вызвать контекстное меню нажатием правой кнопки мыши. В появившемся окне следует выбрать пункт «Просмотр». При этом на экране появляется окно просмотра шаблона (рисунок 87).

Рисунок 87 - Окно просмотра шаблона

7.10. Просмотр событий безопасности

Контролер может просматривать события безопасности:

- собственной сессии;
- сессий администраторов удаленного управления СХСЗ;
- сессий пользователей клиентских устройств.

Указанные события фиксируются в общем журнале и отображаются на вкладке «Журнал событий» (рисунок 53).

Общий журнал хранится в БД (внутренней или внешней, в зависимости от настроек СХСЗ) и не перезаписывается при выключении или перезагрузке как СХСЗ, так и внешней СУБД.

Для поиска нужной информации в событиях можно использовать функцию фильтра, доступную в верхней части окна. Применение фильтра происходит при нажатии на клавишу «Enter», поиск осуществляется с учетом регистра. Для удаления фильтра необходимо удалить искомый текст и вновь нажать клавишу «Enter».

Также есть возможность просмотра события за определенный период. Для использования этой функции нужно выбрать период отображаемых записей в правой части окна и нажать кнопку <Применить>. Доступны следующие варианты:

- за сегодня (по умолчанию);
- за предыдущий день;
- за неделю;
- за месяц;
- за указанный (произвольный) период.

ВНИМАНИЕ! События, отображаемые в журнале, указаны по текущему времени на рабочем месте Контролера, на котором установлена утилита удаленного управления, при этом фильтры по временному периоду работают со временем событий в UTC.

При нажатии кнопки <Экспорт> доступна функция экспорта журнала событий. Экспорт записей производится в соответствии с заданным фильтром по времени в текстовом формате в файл с расширением .txt.

7.11. Восстановление сессии пользователя

В статусной строке главного окна программы удаленного управления СХСЗ отображается индикатор наличия связи с сервером RMQ – желтая надпись «Подключено». Рядом с ней располагается кнопка для проверки подключения (рисунок 78).

В случае если в процессе работы происходит потеря связи с сервером RMQ, цвет индикатора меняется на серый, а сообщение – на «Связь потеряна» (рисунок 79).

Если связь будет восстановлена, то программа автоматически возобновит подключение. Пользователь может проверить наличие подключения вручную, кликнув по кнопке <Проверить подключение>.

В случае потери связи пользователь может просматривать данные, но не может выполнять операции добавления, удаления или редактирования.

7.12. Просмотр информации о продукте и статусе лицензии СХСЗ

Контролер может просматривать информацию о продукте, а также о статусе лицензии на СХСЗ. Подробнее – раздел 4.11.

7.13. Завершение работы ПО управления

Для завершения работы Контролер должен нажать кнопку  в ПО управления СХСЗ и завершить работу с ПО удаленного доступа к СХСЗ.

8. Изменение тайм-аута подключения к RMQ ПО удаленного управления СХСЗ

Интервал подключения к RMQ отображается на вкладке «Устройство Центр-Т» окна «Редактирование пользователя».

По умолчанию интервал подключения rmqAllTimeout для всех команд, кроме получения данных из AD, имеет значение 5 секунд, для команды получения пользователей из AD тайм-аут rmqAdTimeout равен 25 секундам. В случае, если в сети между рабочим местом администратора удаленного управления и СХСЗ присутствуют значительные временные задержки, значения тайм-аутов рекомендуется увеличить. Для внесения соответствующих изменений следует открыть конфигурационный файл

C:\ProgramData\OKB SAPR\Center-T\CTARMOptions.xml

при помощи утилит Блокнот, WordPad, Notepad++ или других текстовых редакторов, позволяющих работать с xml-файлами, и изменить значения «value» для параметров rmqAllTimeout и rmqAdTimeout.

9. Техническая поддержка

В случае необходимости консультации ОКБ САПР предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 17-00 (по московскому времени) обращаться по телефонам

+7 (495) 994-49-96,

+7 (495) 994-49-97,

+7 (926) 235-89-17

или по адресам электронной почты:

support@okbsapr.ru, help@okbsapr.ru.

Наш адрес в Интернете: http://www.okbsapr.ru/

10. Карта информационных потоков взаимодействия сегмента клиентских рабочих мест и сегмента терминальных серверов Citrix

В таблице 3 приведена карта информационных потоков, в которой содержится перечень используемых протоколов и портов взаимодействия сегмента клиентских рабочих мест и сегмента терминальных серверов Citrix.

Таблица 1 – Карта информационных потоков[1]

Идентификатор отправителя	Подсистема отправителя	Идентификатор получателя	Подсистема получателя	Адрес отправителя пакетов	Адрес получателя пакетов	Протокол/порт сетевого взаимодействия
<host A>	<AC A>	<host B>	<AC B>	<1.1.1.1>	<2.2.2.2>	<TCP/UDP:xxxx>
Клиентское устройство (терминальная станция)	Сегмент клиентских рабочих мест	Терминальный сервер Citrix	Сегмент терминальных серверов Citrix	< >	< >	**UPD:1604** (Client-to-server (directed UDP)); **TCP:1494** (ICA sessions (входящий clients to servers)); **TCP:80** (Citrix XML Service)[2]
Терминальный сервер	Сегмент терминальных серверов Citrix	Клиентское устройство (терминальная станция)	Сегмент клиентских рабочих мест	< >	< >	**TCP:1024**
Клиентское устройство (терминальная станция)	Сегмент клиентских рабочих мест	СХСЗ	Сегмент серверов СХСЗ	<>	<>	**TCP:5000 TCP:5672**
СХСЗ	Сегмент серверов СХСЗ	Клиентское устройство (терминальная станция)	Сегмент клиентских рабочих мест	<>	<>	TCP:5000 TCP:5672[3]

[1] Карта информационных потоков составлена с учетом того, что СХСЗ и клиентское устройство расположены в одном сегменте сети.

[2] Порт конфигурируется при установке сервера Citrix XenApp. По умолчанию 80. Можно задать другое значение, например, 8080.

[3] При условии, что используется встроенный в СХСЗ RabbitMQ сервер. При использовании стороннего порт может быть изменен.

Идентификатор отправителя	Подсистема отправителя	Идентификатор получателя	Подсистема получателя	Адрес отправителя пакетов	Адрес получателя пакетов	Протокол/порт сетевого взаимодействия
СХСЗ	Сегмент серверов СХСЗ	PostgreSQL (сервер БД)	Сегмент базы данных	<>	<>	TCP:5432[4]
АРМ (Утилита удаленного управления)	Сегмент администрирования	СХСЗ	Сегмент серверов СХСЗ	<>	<>	TCP:5672[5]

[4] Только при использовании внешней СУБД. Порт по молчанию 5432, но может быть изменен (зависит от конфигурации используемой СУБД).

[5] При условии, что используется встроенный в СХСЗ RabbitMQ сервер. При использовании стороннего порт может быть изменен.

11. Принятые термины и сокращения

АРМ – автоматизированное рабочее место;
БД – база данных;
БИ – безопасность информации;
ОС – операционная система;
ПАК – программно-аппаратный комплекс;
ПИ – персональный идентификатор;
ПО – программное обеспечение;
СВТ – средство вычислительной техники;
СХСЗ – Сервер хранения и сетевой загрузки;
ТС – терминальная станция;
AD – Active Directory.

ПРИЛОЖЕНИЕ 1
НАСТРОЙКА СТРАНИЦЫ AUTOLOGIN ДЛЯ SSO

Настройка механизма SSO выполняется в следующем порядке.

1. На брокере для storefront активировать HTTP Basic аутентификацию.

2. Задать желаемый URL Citrix Receiver-а (Web Interface address). По умолчанию имеет вид https://ip_or_fqdn/Citrix/StoreWeb (например, http://192.168.1.10/Citrix/StoreWeb), но может быть изменен (например, http://192.168.1.10/Citrix/TestWeb)

3. В AutoLogin.html на строке 204 (текст строки window.open("http://ip_or_fqdn/Citrix/StoreWeb");) указать корректное значение URL (Web Interface address).

4. Скопировать AutoLogin.html в каталог сайта брокера citrix. По умолчанию это каталог *C:\inetpub\wwwroot\Citrix\StoreWeb*. Если используется URL не по умолчанию, путь к каталогу будет *C:\inetpub\wwwroot\path\file_name.*

5. Проверить доступность добавленной страницы, открыв в браузере страницу URL/autologin.html (с учетом регистра).

6. Проверить работу механизма Autologin, введя в строке URL/autologin.html?data={"username":"domain\\user","password":"P@ssw0rd"}

ВНИМАНИЕ! После проверки нужно очистить историю страниц браузера (IE или Firefox), чтобы в ней не остался пароль от учетной записи.

При указании в адресе элементов Citrix и StoreWeb следует учитывать, что регистр имеет значение.

domain\\user – имя учетной записи пользователя

P@ssw0rd – пароль пользователя

7. В браузере должна появиться запись "Авторизация успешна..." и произойти перенаправление на страницу брокера.

Примечание: в настоящее время по умолчанию в браузерах блокируются всплывающие окна, поэтому вместо перенаправления может отобразиться запись о заблокированном окне.

Для проверки работы достаточно разрешить открыть всплывающее окно однократно.

Страница SSO по умолчанию поддерживает сессию пользователя активной при помощи KeepAlive сообщений брокеру (раз в 30 секунд). Однако возможны ситуации, при которых данная функция не будет работать корректно (например, при использовании на DNS ALIAS записи для брокера).

В таком случае допускается изменение timeout сессии пользователя со стороны Storefornt (параметр Session timeout, подробнее о настройке – в документации Citrix https://support.citrix.com/article/CTX211564).

ВНИМАНИЕ! Со стороны ПАК СЗИ НСД семейства «Аккорд» необходимо установить параметр AutoLoginSession=Yes и перезагрузить сервер.

ПРИЛОЖЕНИЕ 2
РАБОТА СХСЗ ВЕРСИИ 1.1.8 ВНУТРИ КОНТЕЙНЕРА В ВЕРСИЯХ 1.2.2-1.2.11

1. Общие сведения

Одно из основных отличий «нового» ПАК «Центр-Т» (версии 1.2.0 и выше) от «старого» ПАК «Центр-Т» (версии 1.1.8 и ниже) заключается в технологии, на которой основано хранение, передача и запуск образов ПО ТС.

Так, ПАК «Центр-Т» версии 1.2.2 и выше использует технологию контейнеризации, в то время как ПАК «Центр-Т» версии 1.1.8 и ниже хранит образы ПО ТС на FTP-сервере и передает их на Клиентские устройства по протоколу FTP.

Изменение технологии хранения, передачи и запуска образов ПО повлекло за собой повышение стабильности работы, упрощение работы администраторов Комплекса. Вместе с тем, «новый» ПАК «Центр-Т» накладывает более жесткие условия на терминальные станции, которые могут быть использованы в качестве СХСЗ или клиентских мест.

Начиная с версии 1.2.2 возможно совместное использование ПАК «Центр-Т» новых версий с версией 1.1.8.

ВНИМАНИЕ! Совместная работа ПАК «Центр-Т» новых версий с версией 1.1.8 возможна только в случае использования в качестве СХСЗ Специального носителя Центр-Т 4ГБ, а при включении виртуального СХСЗ необходимым условием является подключение носителя 4ГБ, который ранее использовался в качестве ШИПКА-С 1.1.8.

При использовании версий 1.2.2 - 1.2.11 на СХСЗ должен быть активирован контейнер с СХСЗ версии 1.1.8 (далее – контейнер СХСЗ-1.1.8). Для этого должен быть совершен процесс миграции физического СХСЗ (ШИПКА-С версии 1.1.8) из состава развернутого ПАК «Центр-Т» 1.1.8 в контейнер. ШИПКА-А и ШИПКА-К версии 1.1.8 будут работать в прежнем режиме.

Такой режим работы позволяет использовать ПАК «Центр-Т» версии 1.1.8 для тех рабочих мест, которые не могут быть использованы в рамках «нового» ПАК «Центр-Т».

Перед началом использования ПАК «Центр-Т» версий 1.2.2 - 1.2.11 необходимо составить перечни пользователей:

- которые могут быть переведены на ПАК «Центр-Т» версий 1.2.2 - 1.2.11 (Перечень 1);
- которые могут использовать только Клиентские рабочие места ПАК «Центр-Т» версии 1.1.8 (Перечень 2).

Чтобы пользователь мог быть включен в Перечень 1, он должен удовлетворять следующим условиям:

1) пользователь использует терминал, который поддерживается в качестве Клиентского рабочего места в ПАК «Центр-Т» версий 1.2.2 - 1.2.11 (перечень

ограничений приведен в Сопроводительном письме на ПАК «Центр-Т» версий 1.2.2 - 1.2.11). Следует учесть, что для использования терминала в качестве Клиентского рабочего места необходимо, чтобы процессор этого терминала имел архитектуру x64, а также поддерживал технологию виртуализации. Кроме того, рекомендуется использовать терминалы с объемом RAM от 1Гб.

2) пользователь выполняет подключение к терминальному серверу по протоку ICA.

2. Начало работы с СХСЗ версии 1.1.8 внутри контейнера

Для начала работы с СХСЗ версии 1.1.8 внутри контейнера необходимо выполнить следующие действия:

1) обновить существующую систему до версии 1.1.8, если использовался ПАК «Центр-Т» версии 1.1.7 или ниже;
2) подготовить устройства;
3) смонтировать внешний носитель с образами ПО ТС (загруженные с ШИПКА-С версии 1.1.8) на СХСЗ версий 1.2.2 - 1.2.11;
4) активировать контейнер с СХСЗ 1.1.8.

ВНИМАНИЕ! Действия 1-2 могли быть выполнены ранее, в процессе перехода на ПАК «Центр-Т» версий 1.2.2 - 1.2.11.

2.1. Обновление существующей системы

Если использовался ПАК «Центр-Т» 1.1.7 или ниже, необходимо провести обновление до версии 1.1.8.

Обновление должно быть осуществлено в соответствии с инструкцией из Приложения 1 к сопроводительному письму на ПАК «Центр-Т» 1.1.8.

2.2. Подготовка устройств

Вариант 1. «Новый» ПАК «Центр-Т» ранее не использовался

Дополнительное устройство: USB-устройство (внешний носитель).

В случае если в информационной системе «новый» ПАК «Центр-Т» ранее не использовался, необходимо выполнить следующие действия:

1. Создать резервную копию ШИПКА-С версии 1.1.8.

Действие выполняется в соответствии с разделом 4.6 «Руководства администраторов СХСЗ» для версии 1.1.8.

Резервная копия ШИПКА-С не должна использоваться в дальнейшем и должна храниться в соответствии с внутренними регламентами организации, эксплуатирующей ПАК «Центр-Т».

2. Записать на внешний носитель все образы ПО ТС с ШИПКА-С версии 1.1.8. Действие выполняется в разделе «Управление образами» интерфейса СХСЗ версии 1.1.8.

3. Записать на ШИПКА-С, используемую как СХСЗ версии 1.1.8, образ СХСЗ из состава ПАК «Центр-Т» (при помощи утилиты USBWriter.exe). Обратите

внимание, что перед записью образа не должно происходить повторной инициализации ШИПКА: должны остаться прежние ключи и серийный номер устройства.

4. Записать на все Клиентские устройства пользователей из Перечня 1 образ Клиента из состава ПАК «Центр-Т» версий 1.2.2 - 1.2.11 (при помощи утилиты USBWriter.exe).

Вариант 2. «Новый» ПАК «Центр-Т» уже использовался

В случае если в информационной системе «новый» ПАК «Центр-Т» ранее уже использовался, необходимо выполнить следующие действия:

1. Создать резервную копию ШИПКА-С версии 1.1.8.

Действие выполняется в соответствии с разделом 4.6 «Руководства администраторов СХСЗ» для версии 1.1.8.

Резервная копия ШИПКА-С не должна использоваться в дальнейшем и должна храниться в соответствии с внутренними регламентами организации, эксплуатирующей ПАК «Центр-Т».

2. Записать на внешний носитель все образы ПО ТС с ШИПКА-С версии 1.1.8. Действие выполняется в разделе «Управление образами» интерфейса СХСЗ версии 1.1.8.

3. Если использовалась версия 1.2.1.317, то провести запуск режима отладки на СХСЗ версии 1.2.1.317.

Действие выполняется Администратором сервисного режима СХСЗ в соответствии с подразделом 3.4.

4. Если использовалась версия 1.2.1.317, то провести копирование по scp на СХСЗ версии 1.2.1.317 файла migr_317.sql (входит в комплект поставки ПАК «Центр-Т» версий 1.2.2 - 1.2.11).

5. Если использовалась версия 1.2.1.317, то провести подключение к СХСЗ версии 1.2.1.317 по ssh и выполнение следующих команд:

sudo docker stop CenterT-app

sudo docker cp /tmp/migr_317.sql CenterT-db:/tmp/centert-tmp/

sudo docker exec -it CenterT-db sh –c “psql -U user -d centert -a -f /tmp/centert-tmp/migr_317.sql”

sudo docker start CenterT-app

6. Если использовался ПАК «Центр-Т» версии 1.2.1.317, то создать резервную копию базы данных с СХСЗ из состава «нового» ПАК «Центр-Т».

Действие выполняется Администратором сервисного режима СХСЗ в соответствии с пунктом 3.5.3 настоящего Руководства.

7. Записать на ШИПКА-С, используемую как СХСЗ версии 1.1.8, образ СХСЗ из состава ПАК «Центр-Т» версий 1.2.2 - 1.2.11 (при помощи утилиты USBWriter.exe). Обратите внимание, что перед записью образа не должно

происходить повторной инициализации ШИПКА: должны остаться прежние ключи и серийный номер устройства.

8. Если использовался ПАК «Центр-Т» версии 1.2.1.317, то восстановить базу данных пользователей и их настроек.

Действие выполняется Администратором сервисного режима СХСЗ в соответствии с пунктом 3.5.4 настоящего Руководства.

9. Записать на все Клиентские устройства пользователей из Перечня 1 образ Клиента из состава ПАК «Центр-Т» версий 1.2.2 - 1.2.11 (при помощи утилиты USBWriter.exe).

2.3. Монтирование внешнего носителя с образами ПО ТС, загруженных с ШИПКА-С версии 1.1.8

В процессе выполнения действий по подготовке устройств на внешний носитель были записаны все образы ПО ТС с ШИПКА-С версии 1.1.8.

На внешнем носителе в корневом каталоге необходимо создать директорию «images» и переместить в нее все образы ПО ТС, скопированные в корневой каталог носителя ранее. После этого носитель готов для использования в качестве хранилища образов для контейнерной версии СХСЗ 1.1.8.

Для использования внешнего носителя в качестве хранилища образов ПО ТС для контейнерной версии СХСЗ 1.1.8 нужно подключить устройство к СХСЗ версий 1.2.2 - 1.2.11, после чего Администратор сервисного режима должен перейти во вкладку «Хранилище».

В выпадающем списке необходимо выбрать нужное устройство и нажать кнопку <Монтировать> (рисунок 88).

После этого выбрать пункт «Проброс хранилища» и нажать кнопку <Проброс>.

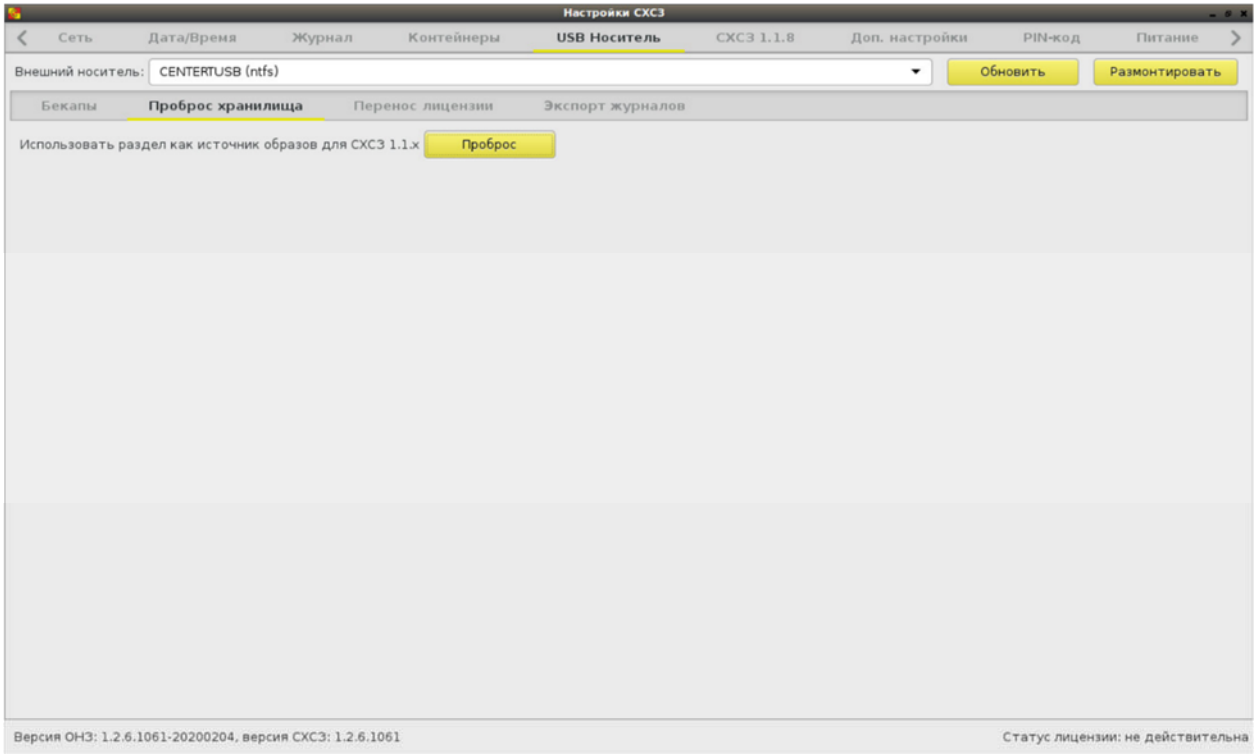


Рисунок 88 - Вкладка «Хранилище»

2.4. Активация контейнера с СХСЗ 1.1.8

Для активации контейнера с СХСЗ 1.1.8 необходимо перейти во вкладку «СХСЗ 1.1.8» и нажать кнопку <Активировать>.

По умолчанию происходит активация контейнера СХСЗ 1.1.8 в режиме автозапуска при старте, то есть после перезагрузки СХСЗ версий 1.2.2 - 1.2.11 контейнер с СХСЗ 1.1.8 будет запущен автоматически.

Автозапуск при старте может быть отключен снятием соответствующего флага в разделе «Конфигурация», после чего обязательно должна быть нажата кнопка <Сохранить> (рисунок 89).

ВНИМАНИЕ! Изменение конфигурации (включение или выключение автозапуска) контейнера СХСЗ 1.1.8 происходит только после его деактивации и последующей активации.

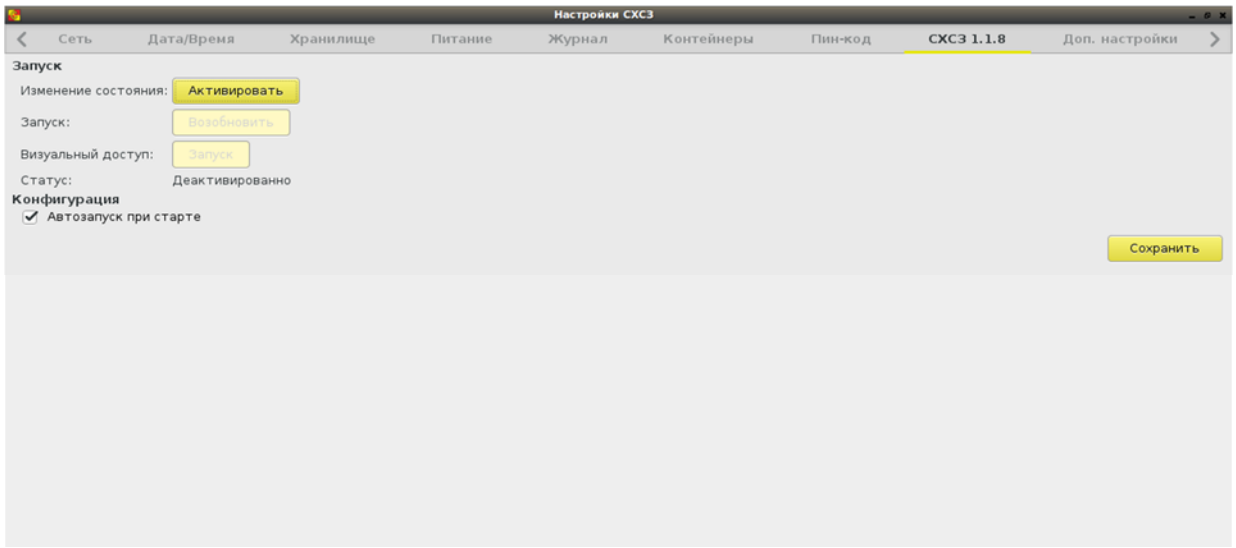


Рисунок 89 - Вкладка «СХСЗ 1.1.8». Флаг «Автозапуск при старте»

После активации контейнера СХСЗ 1.1.8 в поле «Статус» будет отображено значение «Запущен».

После активации пользователи, работающие с ШИПКА-К версии 1.1.8, могут продолжать свою работу без изменений.

3. Получение доступа к СХСЗ 1.1.8 внутри контейнера

Для получения доступа к ПО СХСЗ 1.1.8 внутри контейнера необходимо нажать кнопку <Запуск>, после чего будет открыто окно утилиты «vncviewer» с ПО СХСЗ 1.1.8 внутри контейнера, а именно, окно входа на СХСЗ.

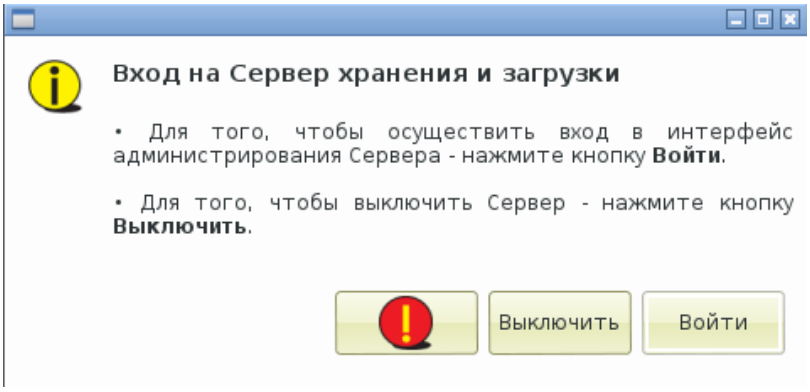


Рисунок 90 - Окно входа на СХСЗ

Для работы с СХСЗ 1.1.8 необходимо нажать на кнопку  и выполнить вход в аварийном режиме (необходимо ввести PIN-код ШИПКА-С).

В дальнейшем работа с СХСЗ 1.1.8 внутри контейнера осуществляется аналогично работе с физической версией ШИПКА-С, за исключением следующих моментов:

1. Работа с ПО СХСЗ 1.1.8 от имени администратора или администратора БИ невозможна при использовании СХСЗ 1.1.8 внутри контейнера. Возможно лишь использование ПО СХСЗ при загрузке в аварийном режиме.

2. При создании пользователей номер идентификатора должен вводиться с клавиатуры.
3. При удаленной работе с СХСЗ 1.1.8 через интерфейс iLO Remote Console любые изменения в настройках контейнера невозможны, доступны только функции запуска и остановки контейнера.

4. Управление работой СХСЗ 1.1.8 внутри контейнера

После активации контейнера СХСЗ 1.1.8 он приобретает статус «Запущено».

В случае если необходимо временно приостановить работу контейнера, следует нажать кнопку <Приостановить>. При этом СХСЗ 1.1.8 продолжает существовать на СХСЗ версий 1.2.2 - 1.2.11, но «поставлен на паузу». Возобновить работу с контейнером можно при нажатии кнопки <Возобновить>.

В случае если необходимо полностью завершить работу контейнера СХСЗ 1.1.8, следует нажать кнопку <Деактивировать>, после чего подтвердить это действие (рисунок 91**Ошибка! Источник ссылки не найден.**). В таком случае контейнер будет полностью удален с СХСЗ версий 1.2.2 - 1.2.11.

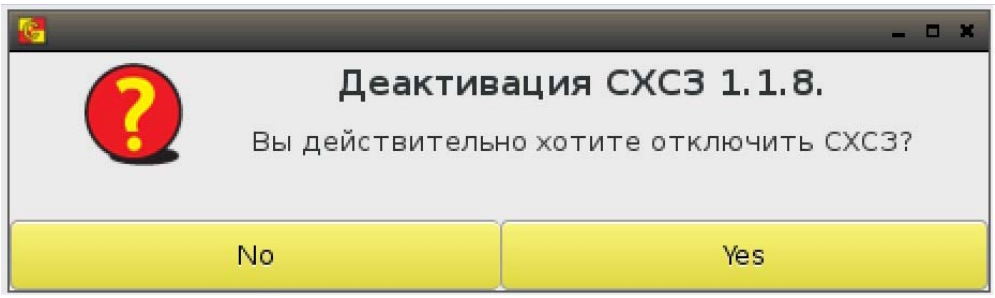


Рисунок 91 - Деактивация СХСЗ 1.1.8

Обратите внимание, что в случае повторной активации СХСЗ 1.1.8 он начнет свою работу в том состоянии и с теми же настройками, которые были сохранены до его активации.

И приостановка, и деактивация делают СХСЗ 1.1.8 недоступным для получения из него назначенных пользователям образов.

ПРИЛОЖЕНИЕ 3
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 4
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 92), 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.

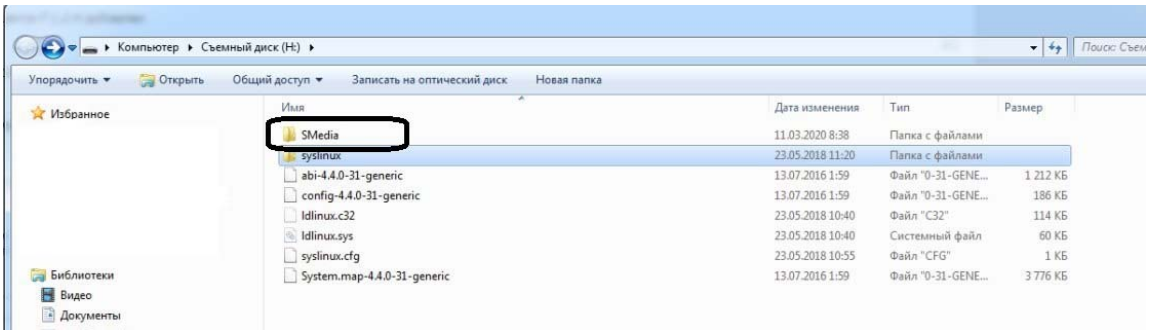


Рисунок 92 – Проводник раздела Специального носителя

После выбора языка (рисунок 93) появится мастер установки ПО (рисунок 94). Следуя его указаниям, выполните процесс установки ПО «Специальный носитель ПО ПАК Центр-Т».

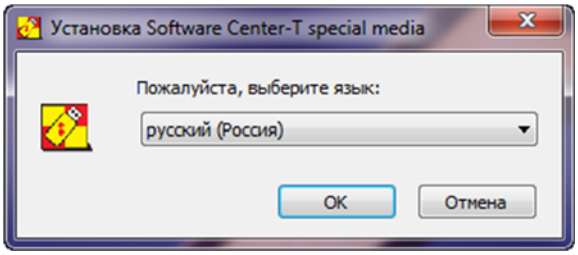


Рисунок 93 – Выбор языка установки ПО

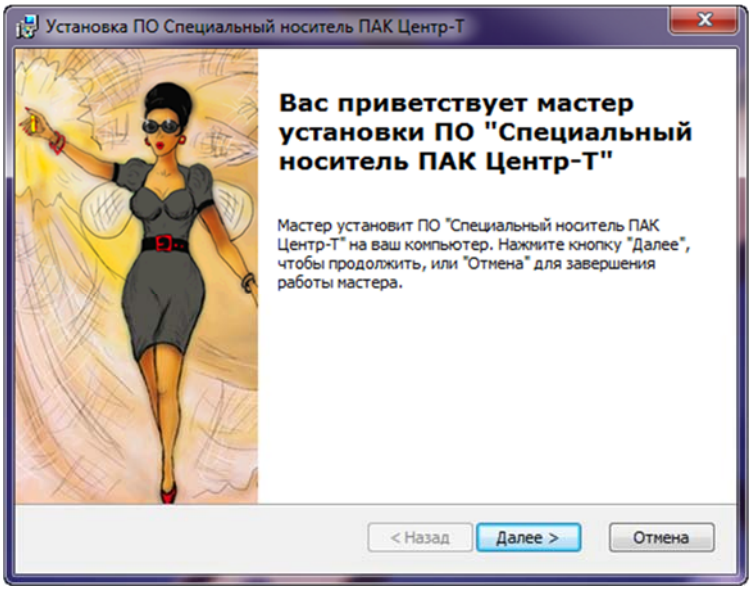
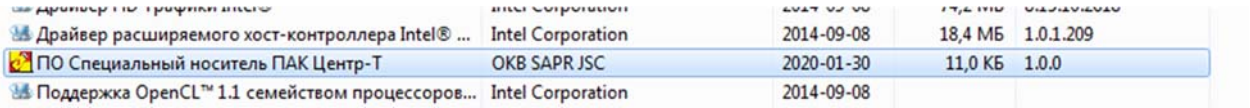


Рисунок 94 – Окно мастера установки ПО

После успешной установки ПО «Специальный носитель ПО ПАК Центр-Т» появится в списке установленных программ и компонентов (рисунок 95).



Драйвер расширяемого хост-контроллера Intel® ...	Intel Corporation	2014-09-08	18,4 МБ	1.0.1.209
ПО Специальный носитель ПАК Центр-Т	OKB SAPR JSC	2020-01-30	11,0 КБ	1.0.0
Поддержка OpenCL™ 1.1 семейством процессоров...	Intel Corporation	2014-09-08		

Рисунок 95 – 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 5
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 6
ИНСТРУКЦИЯ ПО ИЗМЕНЕНИЮ БАЗОВОЙ ДИРЕКТОРИИ СЕРВИСА ОБМЕНА СООБЩЕНИЯМИ RABBITMQ

При использовании RabbitMQ Server на рабочем месте с ОС Windows и необходимости изменить базовую директорию RabbitMQ следует выполнить следующие действия:

1. Через оснастку Службы (Services) остановить службу RabbitMQ и использующие его службы ПАК «Центр-Т», если они используются.
2. Удалить RabbitMQ Server.
3. Переместить конфигурационный файл «rabbitmq.config» из прежней базовой директории (по умолчанию – «%APPDATA@\RabbitMQ») в новую базовую директорию.
4. Установить RabbitMQ Server через пакет rabbitmq-server-X.Y.Z.exe, где X.Y.Z – номер версии. При установке использовать настройки по умолчанию, исключив RabbitMQ Service в диалоге выбора компонентов для установки.
5. Открыть Command Prompt с правами администратора и перейти в директорию sbin, находящуюся в папке установки RabbitMQ.
6. Выполнить команду установки переменной RABBITMQ_BASE, указав базовую директорию RabbitMQ, например, «set RABBITMQ_BASE=C:\ProgramData\RabbitMQData».
7. Выполнить команду установки сервиса RabbitMQ «rabbitmq-service install».
8. Удалить прежнюю папку базовой директории RabbitMQ.
9. Запустить службу «RabbitMQ» через оснастку Службы (Services). Запустить службы ПАК «Центр-Т».

ПРИЛОЖЕНИЕ 7
СОВМЕСТИМОСТЬ МЕЖДУ КОМПОНЕНТАМИ ПАК «ЦЕНТР-Т» РАЗЛИЧНЫХ ВЕРСИЙ

ПАК «Центр-Т» имеет версии формата «1.X.X», где X – числовое значение. Например, «1.3.0». В документации на Комплекс указана версия именно такого формата.

Между тем, каждый компонент ПАК «Центр-Т» имеет собственный номер версии, который можно увидеть в нижней полосе графического интерфейса UI Клиента, СХСЗ (например, рисунок 8), АРМ ЗХСЗ и в окне «О продукте» Утилиты удаленного управления СХСЗ (рисунок 96). Собственный номер версии каждого компонента имеет формат «1.X.Y.Z», где X, Y и Z - числовые значения (например, «1.2.8.1149»). Первые 3 числа в полной записи версии компонента совпадают с версией ПАК «Центр-Т», в состав которого этот компонент входит.

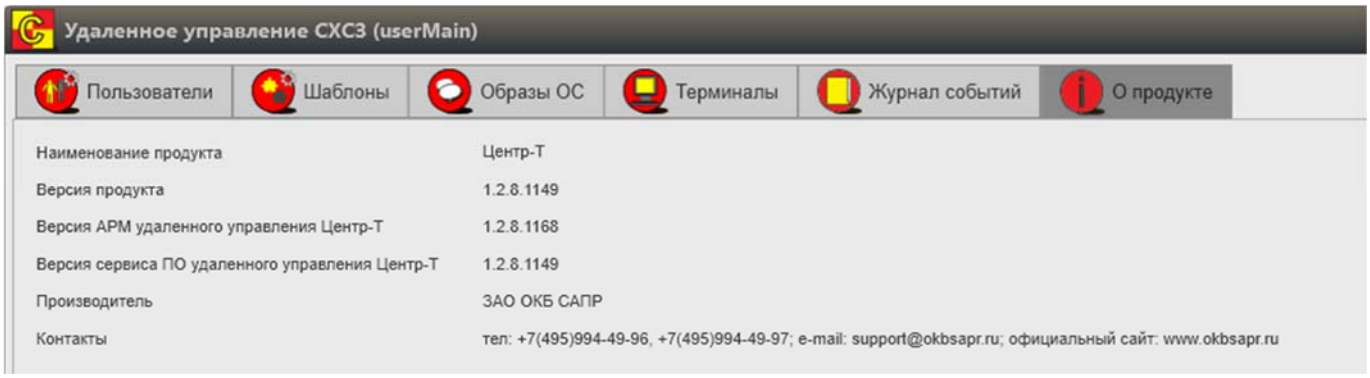


Рисунок 96 – Отображение версий на вкладке «О продукте»

Совместимость между СХСЗ и Клиентом

В ПАК «Центр-Т» реализована возможность работы с компонентами других версий. Так, Клиенты версии «1.2.7.Y» и выше могут подключаться к СХСЗ версии «1.3.0.Y» и выше.

ПРИЛОЖЕНИЕ 8
ИНСТРУКЦИЯ ПО ПЕРЕХОДУ НА ПАК «ЦЕНТР-Т» ВЕРСИИ 1.3.0

Переход на ПАК «Центр-Т» версии 1.3.0 возможен для версий СХСЗ 1.2.7 и выше.

Представлены два варианта перехода на версию 1.3.0 с использованием СКАД «Сигнатура-клиент L» версии 6 и два варианта без ее использования.

Переход на ПАК «Центр-Т» версии 1.3.0 с использованием СКАД «Сигнатура»

Предлагаются примеры перехода с СХСЗ версии 1.2.7 и выше (ОС Ubuntu) на СХСЗ версии 1.3.0 (ОС Debian).

В обоих вариантах для перехода на новую версию необходимо выполнить общие предварительные действия.

Общая подготовка инфраструктуры

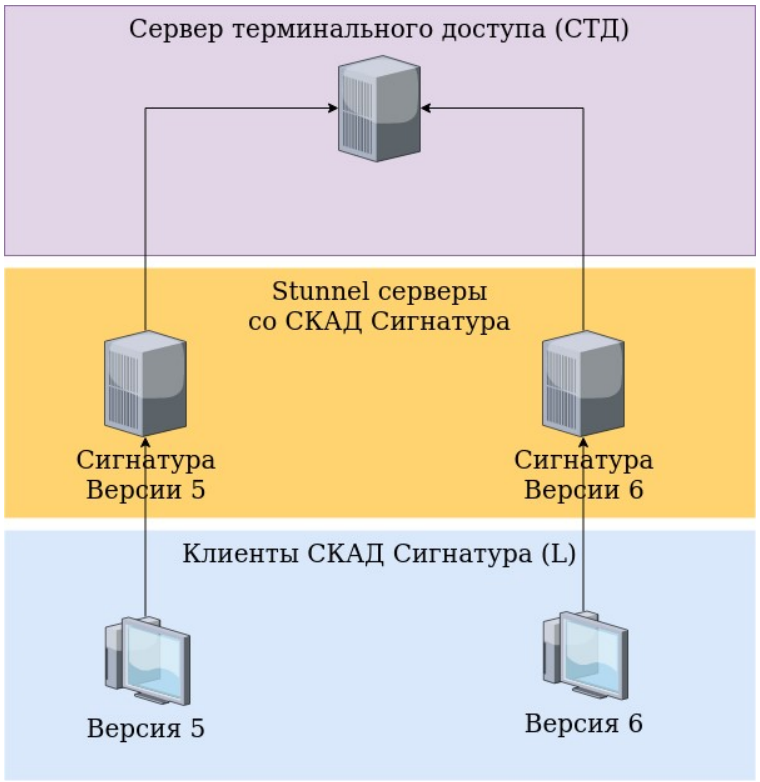


Рисунок 97 - Схема инфраструктуры на этапе подготовки для перехода с использованием СКАД «Сигнатура»

1. Зафиксировать набор пользователей на существующем Stunnel-сервере со СКАД «Сигнатура-клиент L» версии 5, не создавать на нем новых и не удалять старых пользователей.
2. Установить и настроить Stunnel-сервер со СКАД «Сигнатура-клиент L» версии 6.

3. Проверить доступность подключения к нему с помощью СКАД «Сигнатура-клиент L» версии 6 (без использования Клиентов «Центр-Т»).

Вариант 1

В этом примере производится постепенный перевод Клиентов на новый Stunnel-сервер посредством замены внутреннего ПО носителей и переназначения шаблонов.

Вариант характеризуется следующими особенностями:

- Происходит первичная подготовка нового СХСЗ (на базе ОС Debian).
- Затем производится остановка «старого» СХСЗ (на базе ОС Ubuntu) и одновременный ввод в эксплуатацию нового СХСЗ.
- Клиенты продолжают подключаться к «старому» Stunnel-серверу и к новому СХСЗ (Debian).

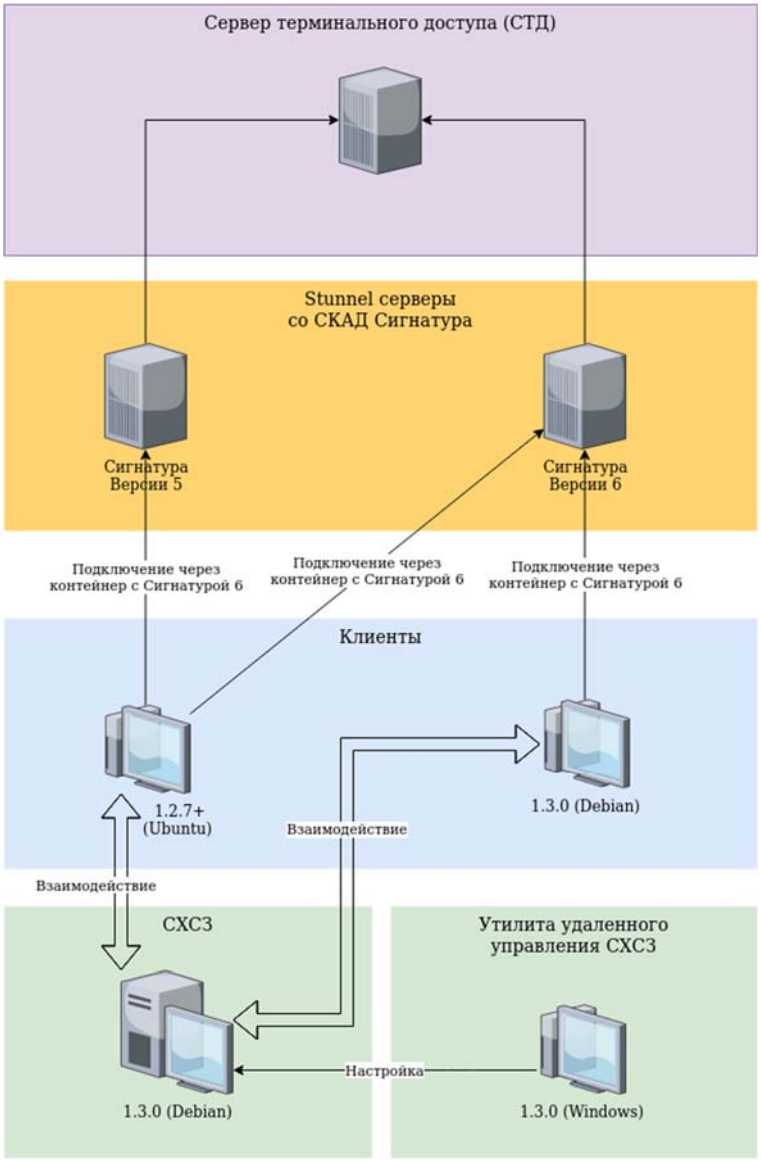


Рисунок 98 - Переход с использованием СКАД «Сигнатура». Вариант 1.

Этап 1:

1. Сделать резервную копию центральной БД на СХСЗ «Центр-Т» 1.2.7+ (Ubuntu) через UI на Linux (подробнее - раздел 3.5 настоящего документа).
2. Запустить новый СХСЗ «Центр-Т» 1.3.0 (Debian) на отдельном IP-адресе (и отдельном RMQ, если используется внешний брокер).
3. В новый СХСЗ (Debian) импортировать центральную БД (через UI на Linux, подробнее - раздел 3.5 настоящего документа). Таким образом все пользователи будут перемещены на новый СХСЗ.
4. Перезагрузить СХСЗ (Debian). После его включения назначенные пользователям контейнеры будут переназначены на их аналоги на базе ОС Debian. С этого момента при подключении к новому СХСЗ (Debian) Клиент получит обновленный контейнер. Однако настройки, указываемые в шаблоне, будут продолжать вести на Stunnel-сервер со СКАД «Сигнатура-клиент L» версии 5, а значит, при запуске контейнера на Клиенте пользователь пока будет подключаться на «старый» сервер (подробнее см. «Руководство по эксплуатации клиентских устройств»).

   В такой комбинации сохраняется возможность использования СКАД «Сигнатура-клиент L» версии 6 со старым шаблоном, т.е. в Клиенте на базе ОС Debian подключаться к «старому» Stunnel-серверу со СКАД «Сигнатура-клиент L» версии 5.
5. С помощью утилиты удаленного управления СХСЗ создать новый Шаблон для подключения к новому Stunnel-серверу со СКАД «Сигнатура-клиент L» версии 6.

Этап 2:

1. Остановить СХСЗ на базе ОС Ubuntu.
2. У нового СХСЗ (Debian) заменить IP-адрес на тот, на котором был развернут «старый» СХСЗ. Это позволит не перенастраивать пользователей (в плане замены настроек IP-адресов подключения).
3. Если используется внешний RMQ, то в настройках нового СХСЗ (Debian) необходимо переключиться на «старый» RMQ.

Этап 3:

1. С помощью утилиты удаленного управления СХСЗ заменить существующий (или добавить новый - для СКАД «Сигнатура-клиент L» версии 6) шаблон для части пользователей. Этот пункт можно производить постепенно, от нескольких до всех (в итоге) пользователей. После такого переназначения при запуске контейнера на Клиенте будут использованы настройки для подключения уже к Stunnel-серверу со СКАД «Сигнатура-клиент L» версии 6.
2. Обновить образы устройств Клиентов на версию ПАК «Центр-Т» 1.3.0 (Debian). Этот пункт тоже можно выполнять постепенно (одновременно с п.1 – сменой шаблона, или отдельно от него).

Этап 4:

1. После перевода всех пользователей ПАК «Центр-Т» на версию 1.3.0 (ОС Debian), в том числе и после переназначения всех шаблонов, можно отключать «старый» Stunnel-сервер со СКАД «Сигнатура-клиент L» версии 5.

Вариант 2

Этот вариант характеризуется следующими особенностями:

- Происходит первичная подготовка нового СХСЗ (на базе ОС Debian).
- Продолжается одновременная работа «старого» и нового СХСЗ.
- Производится постепенный перевод Клиентов на новые версии внутреннего ПО Клиентских устройств, после чего они подключаются только к новому СХСЗ.

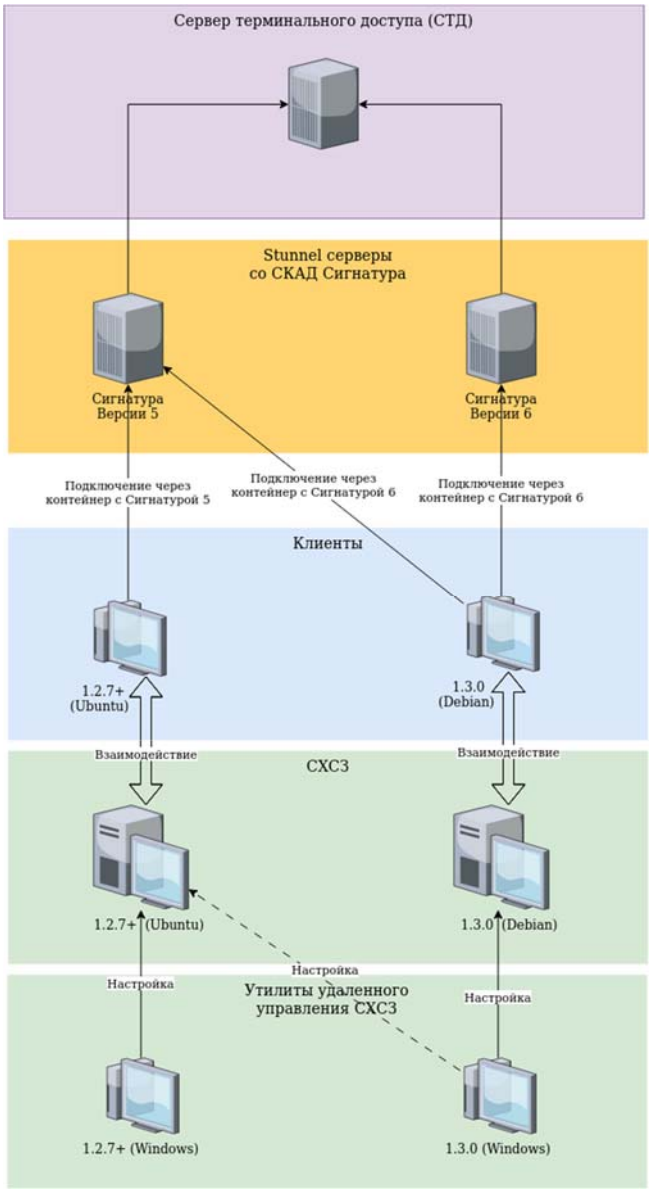


Рисунок 99 - Переход с использованием СКАД «Сигнатура». Вариант 2.

Этап 1:

1. Сделать резервную копию центральной БД на СХСЗ «Центр-Т» 1.2.7+ на базе ОС Ubuntu через UI на Linux.
2. Развернуть новый СХСЗ «Центр-Т» 1.3.0 (Debian) на отдельном IP-адресе (и отдельном RMQ, если используется внешний брокер).
3. В новый СХСЗ (Debian) импортировать центральную БД через UI на Linux.
4. С помощью утилиты удаленного управления СХСЗ создать новый шаблон для подключения к новому Stunnel-серверу со СКАД «Сигнатура-клиент L» версии 6.

Этап 2:

1. Для некоторых (нескольких) пользователей обновить Клиентские устройства на версию ПАК «Центр-Т» 1.3.0 (Debian). В настройках этих устройств указать адрес нового СХСЗ (Debian).
2. Этим пользователям на новом СХСЗ (Debian) назначить новый шаблон для подключения к Stunnel-серверу со СКАД «Сигнатура-клиент L» версии 6.
3. Пункты 1 и 2 можно выполнять постепенно.

Этап 3:

1. После перевода всех пользователей на версию ПАК «Центр-Т» на базе ОС Debian, в том числе и после переназначения всех шаблонов, можно отключать старый Stunnel-сервер со СКАД «Сигнатура-клиент L» версии 5.

Переход на ПАК «Центр-Т» версии 1.3.0 без использования СКАД «Сигнатура»

Предлагаются примеры перехода с СХСЗ версии 1.2.7 и выше (ОС Ubuntu) на СХСЗ версии 1.3.0 (ОС Debian).

Вариант 3

Этот вариант перехода на версию ПАК «Центр-Т» 1.3.0 без использования СКАД «Сигнатура» характеризуется следующими особенностями:

- Происходит первичная подготовка нового СХСЗ (на базе ОС Debian).
- Затем производится остановка «старого» СХСЗ и одновременный ввод в эксплуатацию нового СХСЗ.

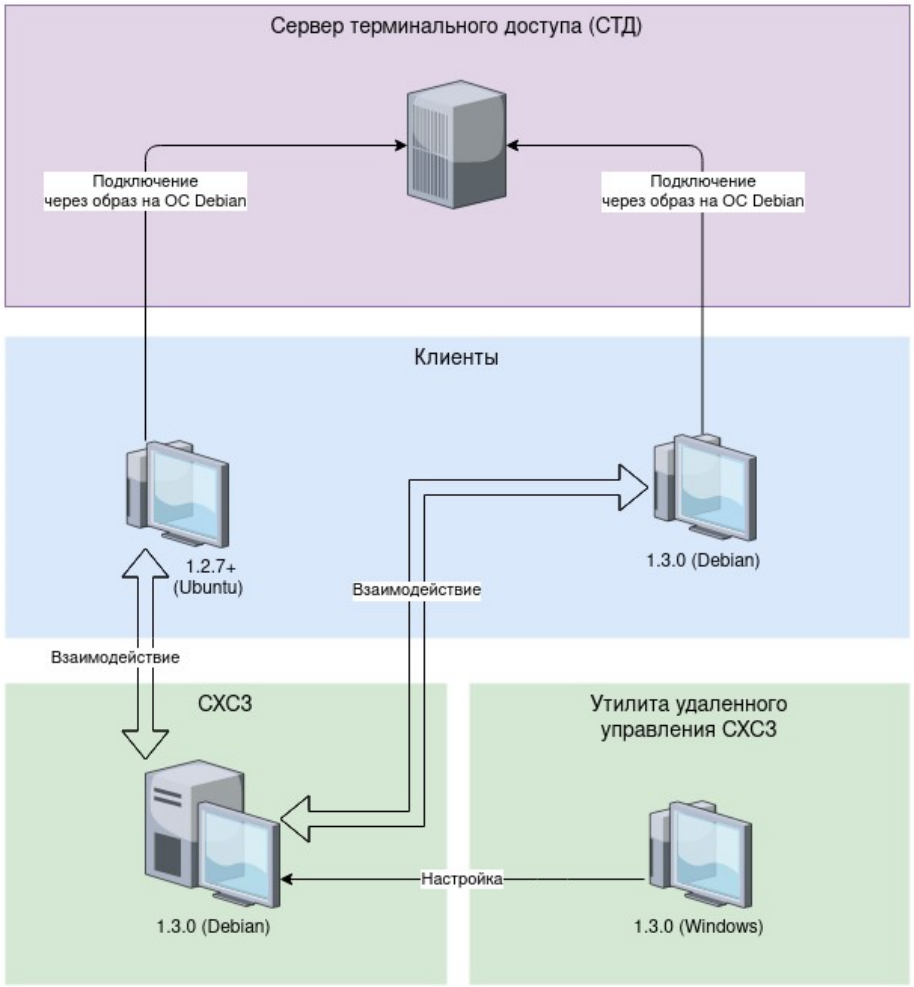


Рисунок 100 - Переход без использования СКАД «Сигнатура». Вариант 3.

Этап 1:

1. Сделать резервную копию центральной БД на СХСЗ «Центр-Т» 1.2.7+ (ОС Ubuntu) через UI на Linux (подробнее - раздел 3.5 настоящего документа).
2. Запустить новый СХСЗ «Центр-Т» 1.3.0 (ОС Debian) на отдельном IP-адресе (и отдельном RMQ, если используется внешний брокер).
3. В новый СХСЗ (ОС Debian) импортировать центральную БД через UI на Linux (подробнее - раздел 3.5 настоящего документа). Таким образом все пользователи будут перемещены на новый СХСЗ.

Этап 2:

1. Остановить СХСЗ на базе ОС Ubuntu.
2. У нового СХСЗ (Debian) заменить IP-адрес на тот, на котором был развернут «старый» СХСЗ. Это позволит не перенастраивать пользователей (в плане замены настроек IP-адресов подключения).
3. Если используется внешний RMQ, то в настройках нового СХСЗ (Debian) необходимо переключиться на «старый» RMQ.

Этап 3:

1. Обновить образы устройств Клиентов на версию ПАК «Центр-Т» 1.3.0 (Debian).

Вариант 4

Еще один вариант перехода на версию ПАК «Центр-Т» 1.3.0 без использования СКАД «Сигнатура». Он характеризуется следующими особенностями:

- Происходит первичная подготовка нового СХСЗ (на базе ОС Debian).
- Продолжается одновременная работа «старого» и нового СХСЗ.
- Производится постепенный перевод Клиентов на новые версии внутреннего ПО Клиентских устройств, после чего они подключаются только к новому СХСЗ.

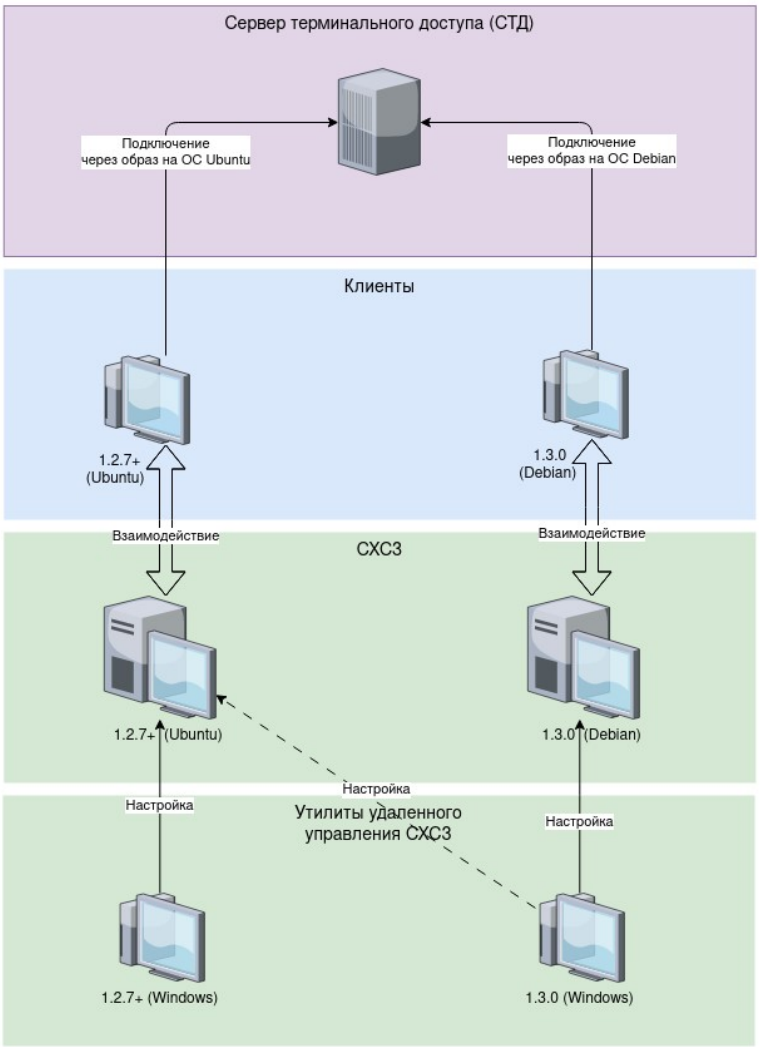


Рисунок 101 - Переход без использования СКАД «Сигнатура». Вариант 4.

Этап 1:

1. Сделать резервную копию центральной БД на СХСЗ «Центр-Т» 1.2.7+ (ОС Ubuntu) через UI на Linux (подробнее - раздел 3.5 настоящего документа).
2. Развернуть новый СХСЗ «Центр-Т» 1.3.0 (Debian) на отдельном IP-адресе (и отдельном RMQ, если используется внешний брокер).
3. В новый СХСЗ (Debian) импортировать центральную БД через UI на Linux.

Этап 2:

1. Для некоторых (нескольких) пользователей обновить Клиентские устройства на версию ПАК «Центр-Т» 1.3.0 (Debian). В настройках этих устройств указать адрес нового СХСЗ (Debian).