

ООО Фирма «ИнфоКрипт»

**ПАК «Сервер безопасности»  
Руководство пользователя**

Москва 2016

1	ВВЕДЕНИЕ	3
1.1	Область применения	3
1.2	Краткое описание возможностей	3
1.3	Перечень эксплуатационной документации	4
2	НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ	5
2.1	Виды деятельности, функции	5
2.2	Программные и аппаратные требования к системе	6
3	ПОДГОТОВКА К РАБОТЕ	7
3.1	Состав дистрибутива	7
3.2	Запуск системы	7
3.3.	Проверка работоспособности системы	13
3.4.	Настройка удаленного доступа	14
4.	КОНФИГУРИРОВАНИЕ	22
4.1.	Управление сетевыми ресурсами	22
4.2.	Управление ключами шифрования	28
4.3.	Управление ключами проверки подписи	30
4.4.	Управление задачами обработки	33
4.5.	Активация конфигурации	37
4.6.	Создание резервной копии конфигурации	38
4.7.	Восстановление конфигурации	38
4.8.	Выгрузка открытого ключа ЭЦП	40
4.9.	Режим параллельной обработки	41
5.	МОНИТОРИНГ	42
5.1.	Просмотр системного журнала	42
5.2.	Просмотр текущего состояния системы	42
5.3.	Остановка системы	42
5.4.	Перезагрузка системы	43
6.	ОБНОВЛЕНИЕ	44
6.1.	Установка обновлений через меню загрузки	44
6.2.	Установка обновлений через меню веб-интерфейса	44
6.3.	Возвращение к предыдущей версии	44
7.	АВАРИЙНЫЕ СИТУАЦИИ	46

## **1 ВВЕДЕНИЕ**

Программно-аппаратный комплекс «Сервер безопасности» (ПАК «СБ») предназначен для обеспечения транзита защищенной информации между различными сегментами локальных сетей в соответствии с предварительно определенным графиком.

### **1.1 Область применения**

ПАК «СБ» рассчитан на применение в локальных сетях стандарта IEEE 802.3, поддерживает межсетевую передачу данных по протоколам CIFS, SMB, NFS, FTP.

### **1.2 Краткое описание возможностей**

ПАК «СБ» предоставляет следующие возможности:

1. Удаленное конфигурирование:
  - настройка расписания задач;
  - определение перечней сетевых ресурсов, ключевых данных.
2. Выполнение задач в соответствии с расписанием:
  - установление соединения с ресурсом-источником, ресурсом-архивом и ресурсом хранения результатов неудачных операций;
  - составление перечня данных в источнике и прием этих данных;
  - архивация принятых данных;
  - обработка принятых данных в соответствии с перечнем операций для данной задачи в расписании;
  - сохранение данных, при обработке которых возникла ошибка;
  - установление соединения с ресурсом-приемником;
  - передача результатов обработки на ресурс-приемник сети.
3. Защита ключевых данных от НСД:
  - шифрование ключевых данных;
  - разграничение прав пользователей системы;
4. Архивация результатов выполнения задач:
  - соединение с ресурсом-хранителем архива;
  - передача результатов обработки данных.
5. Удаленный мониторинг и управление:

- отображение текущего состояния системы (список обрабатываемых в данный момент задач расписания, количество уже обработанных файлов каждой из этих задач);
  - управление выполнением задач – приостановка, отмена, перезапуск.
6. Удаленное обновление.
  7. Восстановление системы после сбоев.

### **1.3 Перечень эксплуатационной документации**

Вместе с ПАК «СБ» поставляется следующая эксплуатационная документация:

- Руководство пользователя ПАК «СБ»

## 2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

### 2.1 Виды деятельности, функции

ПАК «СБ» — это IBM-совместимый компьютер с одним или несколькими сетевыми интерфейсами. Он может подключаться к различным сетевым ресурсам (протоколы SMB, NFS) и сервисам (протоколы FTP) в качестве клиента.

**Основная задача** ПАК «СБ» состоит в том, чтобы, в соответствии с конфигурацией, получить файл из одного сетевого ресурса, обработать его заданным образом и отправить на другой сетевой ресурс.

Обработка файлового ресурса может включать в себя одну или несколько операций из следующего списка:

- преобразование формата;
- архивирование/ разархивирование;
- шифрование/ расшифрование;
- формирование/ проверка ЭЦП;
- формирование/ проверка кодов аутентификации.

Обработка почтового ресурса представлена следующими действиями:

- над вложениями: те же действия, что и над файловыми ресурсами, приводящие к созданию нового почтового сообщения, где вложением является результат обработки исходного вложения;
- над содержимым писем: шифрование/расшифрование, формирование/проверка ЭЦП, формирование/проверка кодов аутентификации.

Таким образом, ПАК «СБ» играет роль многофункционального файлового и почтового шлюза.

Задача ПАК «СБ» определяется следующими параметрами:

- имя задачи;
- ресурс-источник;
- ресурс-приемник;
- перечень операций над данными;
- ключи для операций над данными;
- расписание выполнения;
- ресурс архивации;

- ресурс хранения результатов неудачных операций;
- приоритет;

Ресурс определяется следующими параметрами:

- имя ресурса;
- URL;
- сетевой транспорт;
- имя пользователя для подключения;
- пароль для подключения;
- таймаут подключения.

Ключи шифрования также имеют параметр-имя. Открытые ключи проверки подписи определяются именем и принадлежностью к определенной базе открытых ключей.

## **2.2 Программные и аппаратные требования к системе**

Для функционирования ПАК «СБ» необходимы:

- одно или несколько Ethernet-подключений;
- наличие на доступных по сети узлах ресурсов SMB, NFS, открытых для удаленного доступа, или серверов FTP;
- набор файлов, содержащих конфигурационные параметры системы.

## 3 ПОДГОТОВКА К РАБОТЕ

### 3.1 Состав дистрибутива

Аппаратное обеспечение ПАК «СБ» составляет системный блок с установленными USB-считывателем ТМ, адаптерами сетевых интерфейсов, адаптером видеointерфейса.

Программное обеспечение ПАК «СБ» представляет собой установленную ОС Linux, ПО ПАК «СБ», средства ключевания.

В состав дистрибутива входят также два ТМ-носителя (touch memory) для хранения ключевой информации:

- ТМ-носитель для последующей записи основной копии ключа офицера безопасности;
- ТМ-носитель для последующей записи на него ключа удаленного администратора (с наклейкой «АДМ», см. 3.2.5.4).

Также для надежности и возможности восстановления конфигураций рекомендуется дополнительно иметь два ТМ-носителя, на один из которых записать резервную копию ключа офицера безопасности, а на другой - ключ резервных копий.

### 3.2 Запуск системы

#### 3.2.1 Последовательность действий при загрузке ПАК «СБ»

Содержание процесса загрузки ПАК «СБ» различается для случаев первого запуска и всех последующих.

##### 3.2.1.1 Первый запуск системы

На этот момент система не содержит конфигурационных данных, кроме настроенного комплекса доверенной загрузки ОС.

Загрузка системы завершается отображением окна, в верхней области которого отражены сведения о состоянии системы, а в нижней – меню возможных действий.

В меню доступны пункты:

- «Login & configure» – настройка параметров системы;
- «Reboot» – перезагрузка системы;
- «Turn off» – выключение системы.

В случае первого запуска необходимо установить параметры системы, выбрав пункт меню «Login & configure».

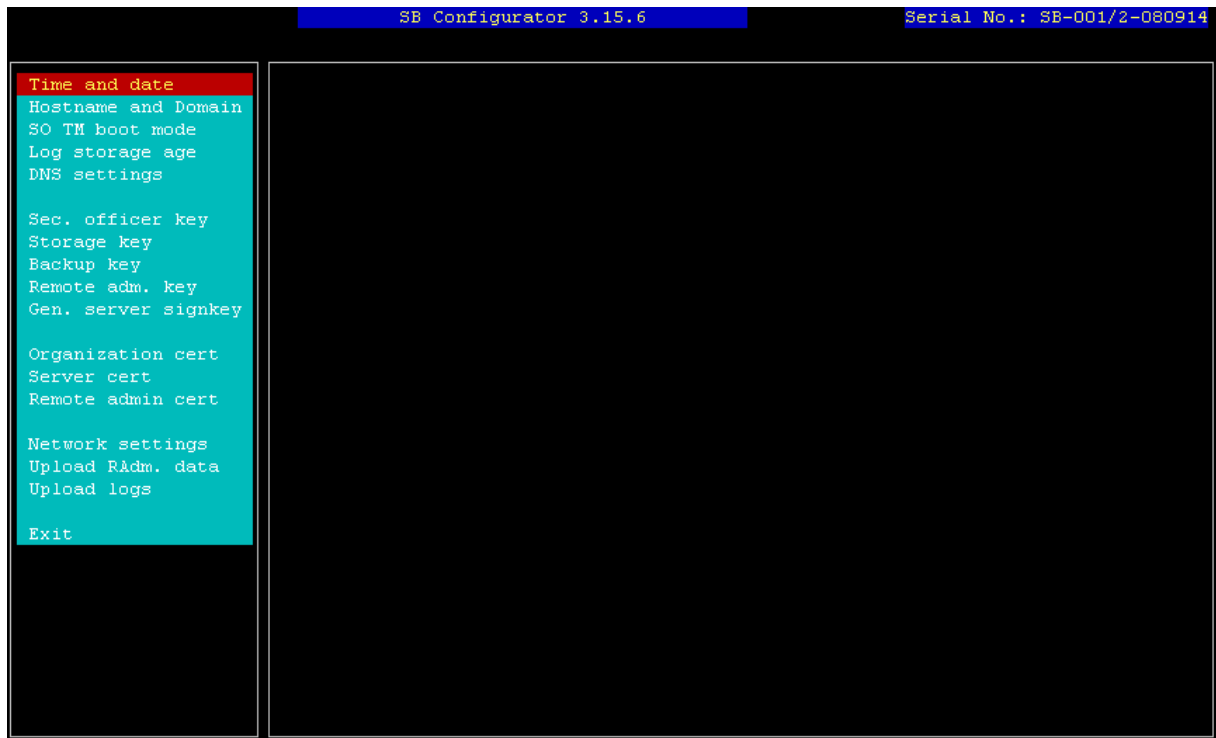


Рис. 1. Окно конфигуратора локальной консоли управления

В новом окне (рис. 1) отображаются следующие пункты меню, из которых пп.1-4,9-17 при **первом запуске** системы необходимо выполнить в строгой последовательности, заполняя **каждое** поле в отображаемых диалоговых окнах:

- 1) установка текущего времени и даты
- 2) установка сетевого имени и домена
- 3) установка режима работы с ключом ОБ (после генерации ключей ОБ и РК путем ввода Yes в ответ на вопрос, выдаваемый при активации данного пункта меню, возможно отключить запрос на приложение ТМ ОБ при загрузке ПАК СБ)
- 4) настройка срока хранения системных логов
- 5) установка адресов сервера DNS
- 6) создание ключа офицера безопасности
- 7) создание ключа хранения
- 8) создание ключа резервного копирования
- 9) создание ключей удаленных администраторов
- 10) создание секретного ключа подписи сервера
- 11) создание сертификата организации
- 12) создание сертификата сервера
- 13) создание сертификатов удаленных администраторов



- 14) настройка параметров сетевых интерфейсов для подключения к глобальной и локальной сетям
- 15) снятие ключевых данных удаленных администраторов на USB-совместимый носитель (при помощи ключевых данных удаленных администраторов становится возможным взаимодействие с веб-интерфейсом конфигурирования системы с удаленного рабочего места для управления задачами (см. 3.4.))

Примечание: для систем с RAID (с двумя жесткими дисками) необходимо, чтобы USB носитель имел метку файловой системы **PAKSB**.

- 16) снятие системных логов на флеш-диск

Выберите пункт меню «Exit» для возврата к основному интерфейсному окну по завершении ввода параметров системы.

### 3.2.1.2 Последующие запуски системы

Параметры системы должны были быть определены ранее.

В ответ на приглашение необходимо приложить к считывателю ТМ-носитель с ключом офицера безопасности для продолжения загрузки системы (ТМ-носитель с наклейкой «ОБ»).

Загрузка системы завершается отображением окна, в верхней области которого отражены сведения о состоянии системы, а в нижней – меню возможных действий.

По окончании загрузки система находится в работоспособном состоянии и готова выполнять возложенные на нее задачи в соответствии с расписанием. Параметры системы можно изменять при помощи Конфигуратора с локальной консоли управления, а также через веб-интерфейс удаленных администраторов.

### 3.2.2 Создание сертификата организации

Сертификат организации является основным сертификатом, используемым в системе удаленного доступа к серверу ПАК «СБ». Им подписываются сертификат сервера и сертификаты удаленных администраторов. Сертификат организации должен присутствовать в хранилище доверенных корневых центров сертификации на всех рабочих местах, с которых планируется осуществлять удаленный доступ к серверу ПАК «СБ».

Выработка сертификата организации осуществляется при первом запуске сервера ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Organization cert**», заполнить необходимые информационные поля и нажать на кнопку «**Save**».

### 3.2.3 Замена сертификата организации

Процедура замены сертификата организации может быть плановой или срочной (в результате каких-либо непредвиденных обстоятельств).

Действия при плановой замене:

1. В течение месяца до истечения срока действия старого сертификата всем администраторам ПАК «СБ» необходимо сменить сертификат организации.
2. Один из администраторов ПАК «СБ» создает штатными средствами новый сертификат организации.
3. Система подписывает существующий запрос на сертификат ПАК «СБ» (либо созданный ранее новый запрос, если предполагается также замена сертификата сервера ПАК «СБ») новым сертификатом организации, тем самым создавая новый сертификат сервера ПАК «СБ», но пока не заменяет им старый. Также сохраняется отпечаток нового сертификата сервера ПАК «СБ».
4. Администратор создает штатными средствами свой новый сертификат для удаленного доступа к серверу ПАК «СБ», подписанный новым сертификатом организации.
5. Администратор забирает с собой на USB-совместимом носителе информации:
  - новый сертификат организации;
  - отпечаток сертификата сервера, подписанного новым сертификатом организации;
  - свой новый сертификат для удаленного доступа.
6. Все остальные администраторы должны выполнить пункты 4 и 5 в течение месяца до истечения срока действия старого сертификата, иначе удаленный доступ будет заблокирован.
7. По истечении срока действия старого сертификата организации, администратор на своем удаленном рабочем месте удаляет старый, недействительный сертификат организации и свой старый сертификат, после чего устанавливает новые сертификаты.

По истечении срока действия старого сертификата организации на ПАК «СБ» происходят следующие замены: старый сертификат организации меняется на новый, секретный ключ организации меняется на новый, старый сертификат сервера меняется на новый, и старый секретный ключ сервера меняется на новый. С этого момента удаленный доступ к серверу ПАК «СБ» по сертификатам администраторов, подписанным старым сертификатом организации, будет прекращен. Для доступа будет

необходимо пользоваться новыми сертификатами. Проверку отпечатка сертификата сервера также нужно будет проводить по новому образцу.

Действия при возникновении непредвиденных обстоятельств (компрометация и т.д.) те же, что и при плановой замене, но срок действия старого сертификата может быть сокращен согласно внутреннему регламенту организации.

### 3.2.4 Создание сертификата сервера

Сертификат применяется в системе удаленного доступа к серверу ПАК «СБ». В процессе аутентификации удаленному администратору предъявляется сертификат сервера. Удаленный администратор обязан сверить отпечаток предъявленного сертификата с эталонным отпечатком сертификата сервера, который был ему предоставлен при получении собственного сертификата (сертификата администратора).

Выработка сертификата сервера осуществляется при первом запуске ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Server cert**», заполнить необходимые информационные поля и нажать на кнопку «**Save**».

### 3.2.5 Создание сертификата удаленного администратора

Сертификат применяется в системе удаленного доступа к серверу ПАК «СБ». В процессе установки закрытого канала связи с сервером ПАК «СБ» применяется двухфакторная аутентификация. Сертификат удаленного администратора предъявляется серверу, который его проверяет и разрешает удаленное соединение, если проверка проходит успешно. Сертификат удаленного администратора должен находиться в личном хранилище сертификатов на рабочем месте администратора.

Выработка сертификата удаленного администратора осуществляется при первом запуске ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Remote admin cert**», выбрать удаленного администратора из списка, заполнить необходимые информационные поля и нажать на кнопку «**Save**».

## 3.2.6 Выработка ключевых данных

### 3.2.6.1 Выработка ключа Офицера Безопасности

**Ключ Офицера Безопасности (Коб)** – ключ, на котором зашифрованы ключ хранения на жестком диске и ключ хранения резервных копий. Ключ содержится на touch memory (ТМ) носителе, вырабатывается в одном или двух экземплярах (на одном/двух ТМ-носителях). Основная копия записывается на ТМ-носитель с наклейкой «ОБ», который поставляются вместе с ПАК «СБ».

Основная копия отдается на хранение офицеру безопасности. Резервная копия (если создана) должна храниться в защищенном месте с ограниченным доступом (меры предосторожности определяются внутренним регламентом организации).

Выработка *Коб* осуществляется при первом запуске сервера ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Sec. officer key**», затем подпункт «**Create new**», и далее следовать инструкции на экране.

### 3.2.6.2 Выработка ключа хранения на жестком диске

**Ключ хранения на жестком диске (Кз)** – ключ, на котором зашифрованы данные на жестком диске. Используется для шифрования/расшифрования защищенной области диска. Ключ *Кз* зашифрован на *Коб*. При включении ПАК «СБ» требуется предъявить *Коб*, на котором расшифруется *Кз*, на котором, в свою очередь, расшифруется защищенная область диска.

Выработка *Кз* осуществляется при первом запуске ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Storage key**» и далее следовать инструкции на экране.

### 3.2.6.3 Выработка ключа хранения резервных копий (не обязательно)

**Ключ хранения резервных копий (Крк)** – ключ, на котором шифруются резервные копии настроек сервера ПАК «СБ». Вырабатывается в двух экземплярах. Основная копия хранится в зашифрованном на *Коб* виде на жестком диске. Резервная копия ключа хранится на ТМ-носителе в месте с ограниченным доступом (определяется внутренним регламентом организации). Если при восстановлении данных из резервной копии *Крк* оказывается недоступен с жесткого диска, то его можно импортировать с ТМ-носителя через меню конфигуратора локальной консоли управления (см. 4.8). Обратите внимание: если этот ключ не создан, ПАК «СБ» будет работать нормально, однако создание/восстановление резервных копий конфигурации будет невозможно.

Выработка *Крк* осуществляется при первом запуске ПАК «СБ». Для этого необходимо в меню конфигуратора выбрать пункт «**Backup key**», подпункт «**Create new**» и далее следовать инструкции на экране.

В случае плановой или срочной замены *Коб* существующий *Крк* заново шифруется на новом *Коб*. Чтобы и в дальнейшем обеспечить возможность восстановления сделанных ранее резервных копий конфигурации ПАК «СБ» (см. 4.7, 4.8), резервную копию *Крк*, зашифрованного на новом *Коб*, нужно записать на ТМ-носитель. Для этого нужно выбрать пункт меню конфигуратора «**Backup key**», затем подпункт «**Upload Existing**», и следовать инструкции на экране.

### 3.2.6.4 Выработка ключа удаленного администратора

**Ключ удаленного администратора (Кадм)** – ключ для шифрования и подписи данных перед отправкой их с удаленного рабочего места на сервер ПАК «СБ».

Выработка *Кадм* осуществляется при первом запуске ПАК «СБ». Для этого необходимо в меню configurатора выбрать пункт «**Remote adm. key**» и далее следовать инструкции на экране. Ключ удаленного администратора записывается на ТМ-носитель с наклейкой «АДМ», который поставляется вместе с ПАК «СБ».

### 3.2.7. Конфигурация сетевых подключений

Выбор пункта «**Network settings**» в меню configurатора позволяет определить настройки подключения по сетевым интерфейсам, сетевые маршруты, а также параметры подключения web-сервера и по ssh.

Для каждого сетевого интерфейса задаются его ip-адрес и маска подсети в случае статического назначения, либо, в случае динамического, необходимо в поле ip-адреса ввести DHCP.

Для конфигурирования подключения к web-серверу ПАКСБ необходимо указать ip-адрес и порт на том интерфейсе, по которому осуществляется подключение к web-интерфейсу управления ПАКСБ, например: 192.168.3.1:443.

Для конфигурирования подключения к ПАКСБ по ssh необходимо указать его ip-адрес интерфейса, по которому организуется это подключение, например: 192.168.3.1. Подключение по умолчанию выполняется по порту 22.

Также средствами этого пункта configurатора возможно задать дополнительные сетевые маршруты. Для этого необходимо указать в соответствующих полях значения подсети, маски, шлюза и интерфейса, затем перевести фокус на «+» и добавить такой маршрут нажатием Enter.

## 3.3. Проверка работоспособности системы

Переход системы в работоспособное состояние по завершении процесса загрузки характеризуется:

- отображением окна мониторинга на локальной консоли управления (в случае отсутствия обрабатываемых задач или каких-либо проблем в списке задач отображается надпись «no active tasks»);
- началом обработки задач в соответствии с расписанием (при отсутствии каких-либо проблем в список задач включаются записи в соответствии с политикой мониторинга);
- отображением пунктов меню веб-интерфейса удаленного администрирования (после настройки удаленного доступа).

### 3.4. Настройка удаленного доступа

Для осуществления удаленного доступа к серверу ПАК «СБ» администратор должен иметь сертификат организации, а также заверенный им собственный сертификат. Оба сертификата администратор формирует на сервере с помощью меню локального конфигурирования. Затем, посредством того же меню, администратор забирает их на USB-совместимом носителе информации. Сертификат организации импортируется в PEM формате. Сертификат администратора – в формате PKCS#12.

#### 3.4.7. Установка сертификата организации.

1. При помощи любого файлового менеджера найдите на носителе, содержащем сертификаты, файл с сертификатом организации **org.crt** и активируйте процесс установки, открыв этот файл (двойным щелчком левой кнопкой мыши или нажатием клавиши «Ввод»). Появляется следующее окно-предложение (рис. 2):

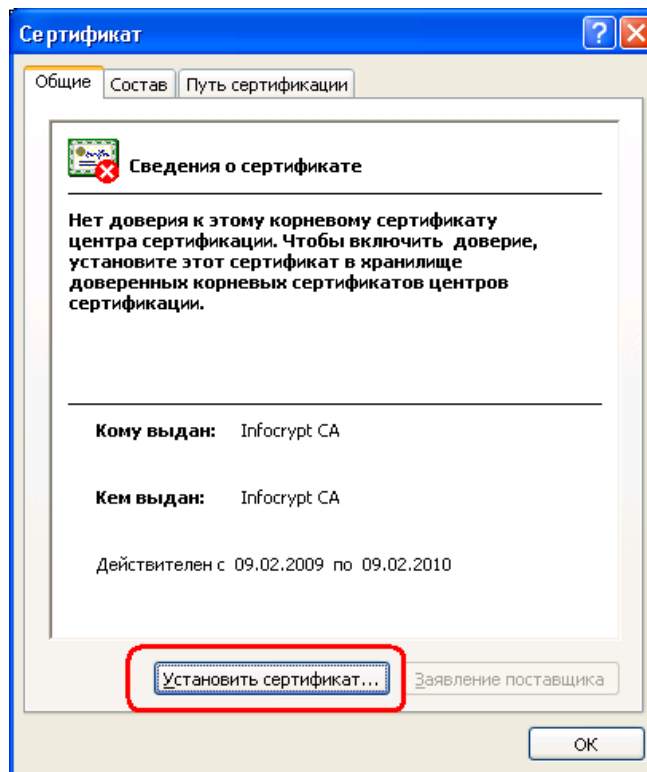


Рис. 1

2. Выберите пункт «Установить сертификат». Запустится мастер импорта сертификатов (рис. 3).

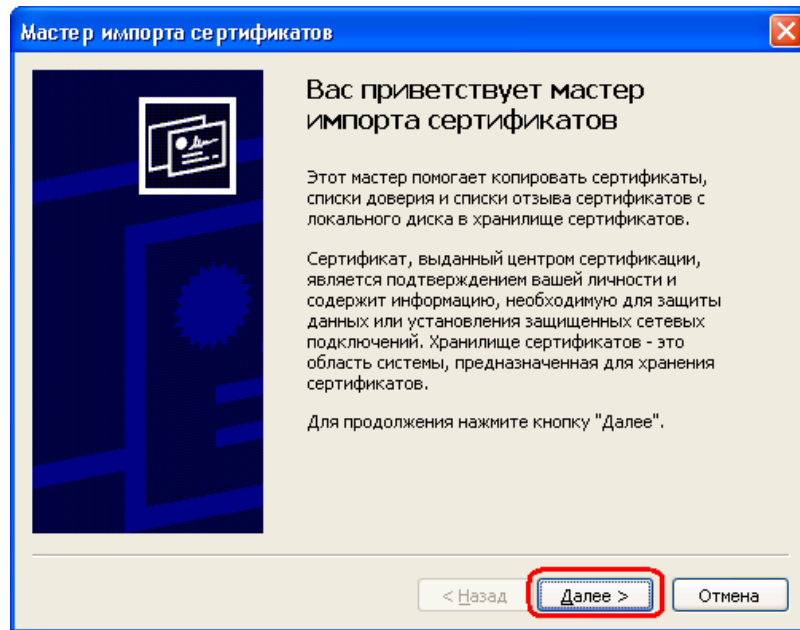


Рис. 3

3. Нажмите на кнопку «Далее». Появится предложение о выборе хранилища для сертификата (рис.4):

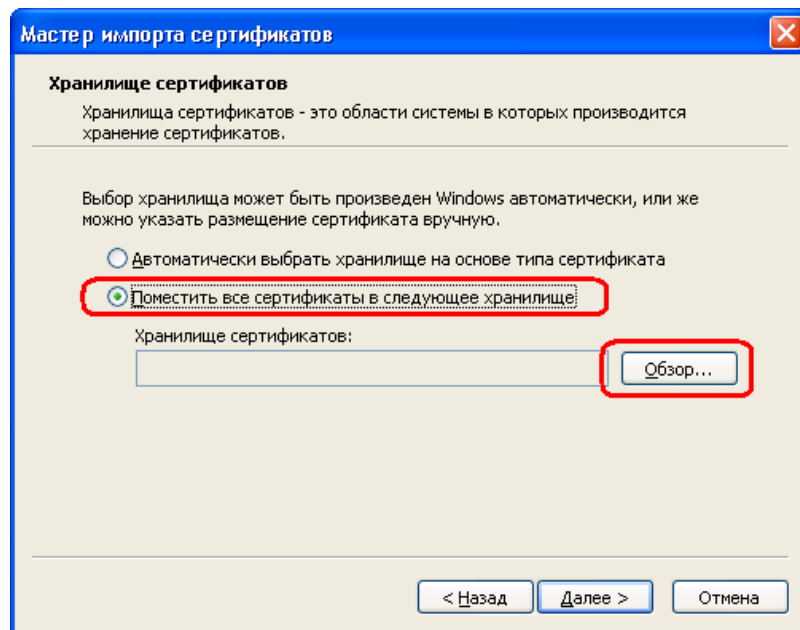


Рис. 4

4. Выберите пункт «Поместить все сертификаты в следующее хранилище». Нажмите на кнопку «Обзор». Появится окно выбора хранилища (рис 5).

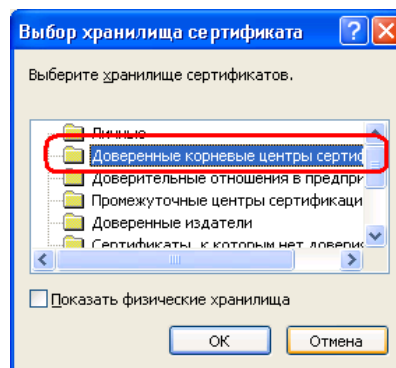


Рис. 5

5. Выберите пункт «Доверенные корневые центры сертификации» и нажмите на кнопку «ОК». Затем нажмите на кнопку «Далее» (рис. 6).

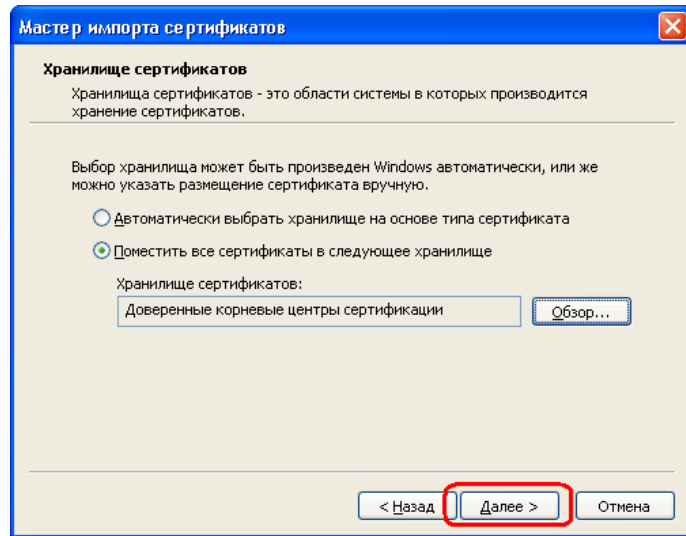


Рис. 6

6. Мастер импорта сертификатов завершает работу (рис. 7). Нажмите на кнопку «Готово».

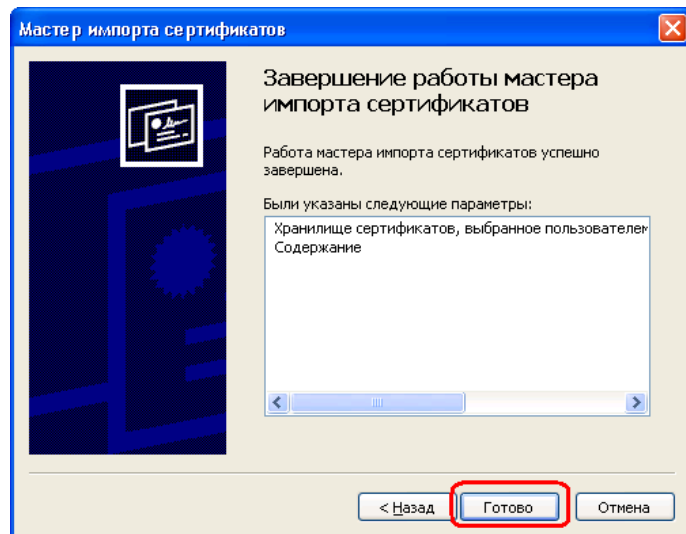


Рис. 7

7. Появится предупреждение системы безопасности. Нажмите на кнопку «Да».

Теперь импорт сертификата организации успешно завершён, о чем операционная система выдает соответствующее сообщение. Посмотреть установленный сертификат организации можно, например, с помощью браузера Internet Explorer, выбрав в свойствах обозревателя вкладку «Содержание», и на ней нажав на кнопку «Сертификаты» (рис. 8).



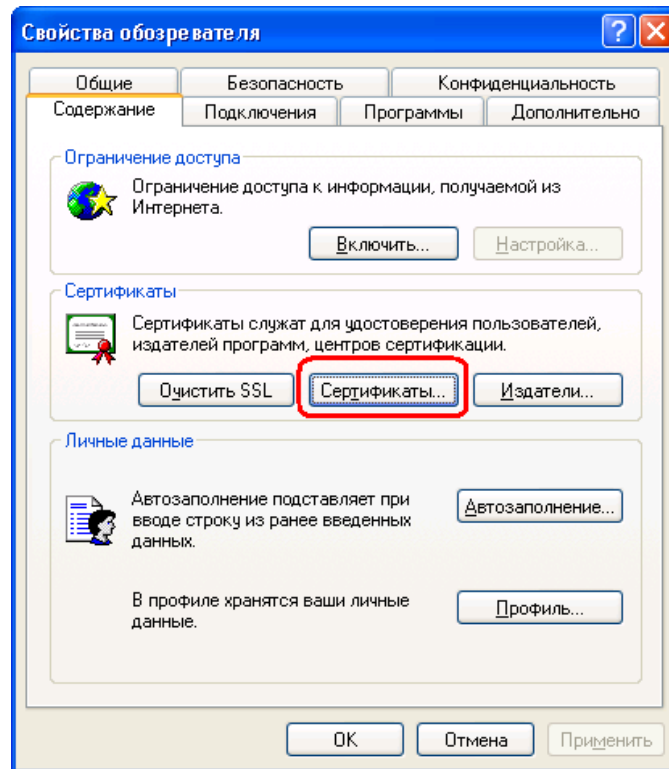


Рис. 8

### 3.4.8. Установка сертификата администратора.

- 1 При помощи любого файлового менеджера найдите на носителе, содержащем сертификаты, файл со своим сертификатом **AdminName.p12** (**AdminName** – имя удаленного администратора) и активируйте процесс установки, открыв этот файл (двойным щелчком левой кнопкой мыши или нажатием клавиши «Ввод»). Запустится мастер импорта сертификатов (рис. 9):

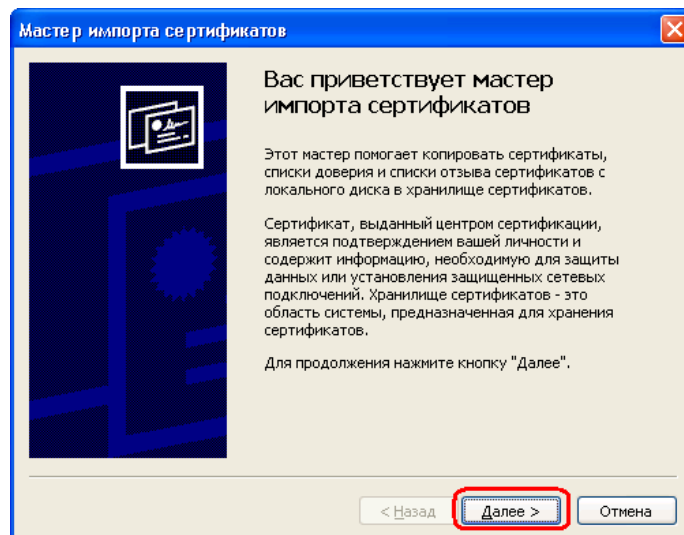


Рис. 9

- 2 Нажмите на кнопку «Далее». В открывшемся окне подтвердите выбранный файл с сертификатом, вновь нажимая на кнопку «Далее» (рис. 10).

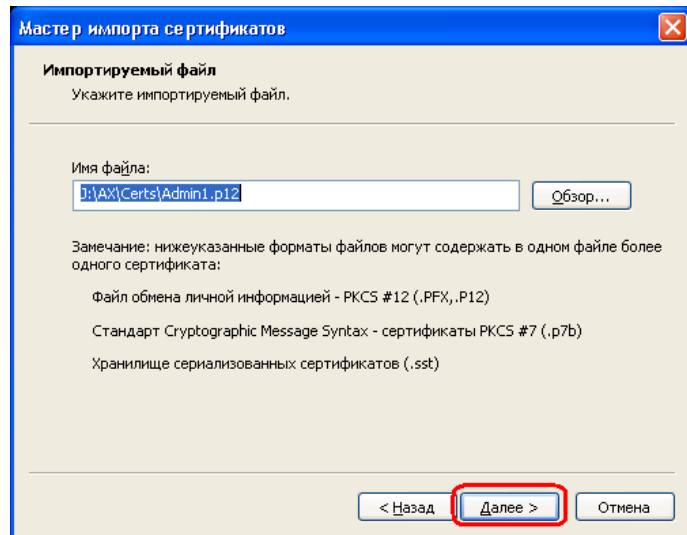


Рис. 10

- 3 Следующее окно предложит ввести пароль секретного ключа. Введите пароль и нажмите на кнопку «Далее» (рис. 11).

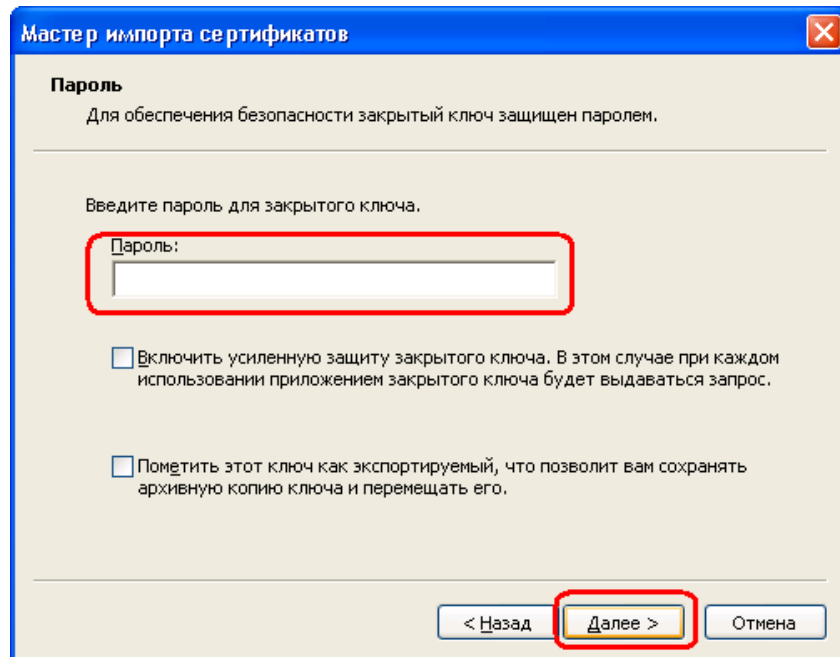


Рис. 11

- 4 Выберите хранилище сертификатов. Нужно отметить пункт «Автоматически выбрать хранилище на основе типа сертификата». Нажмите на кнопку «Далее» (рис. 12).

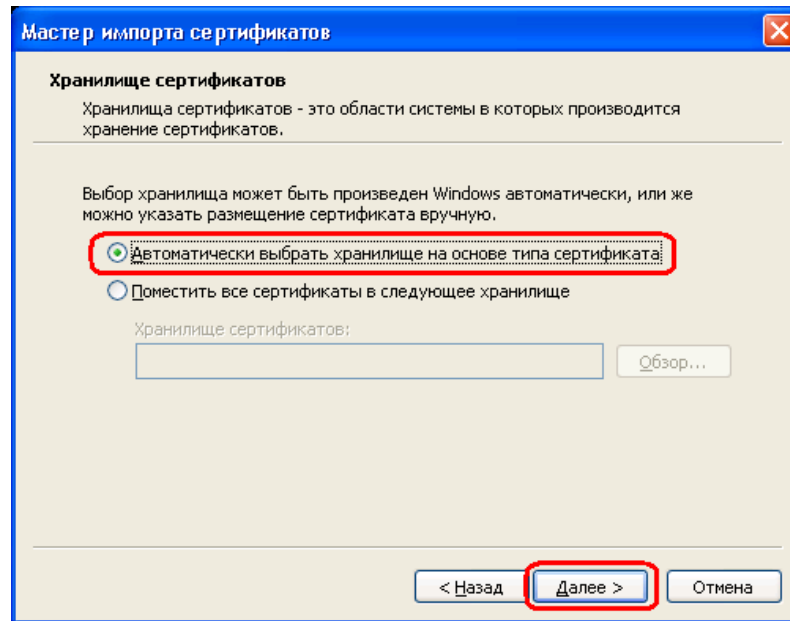


Рис. 12

5 Мастер импорта сертификатов завершает свою работу. Нажмите на кнопку «Готово» (рис. 13).

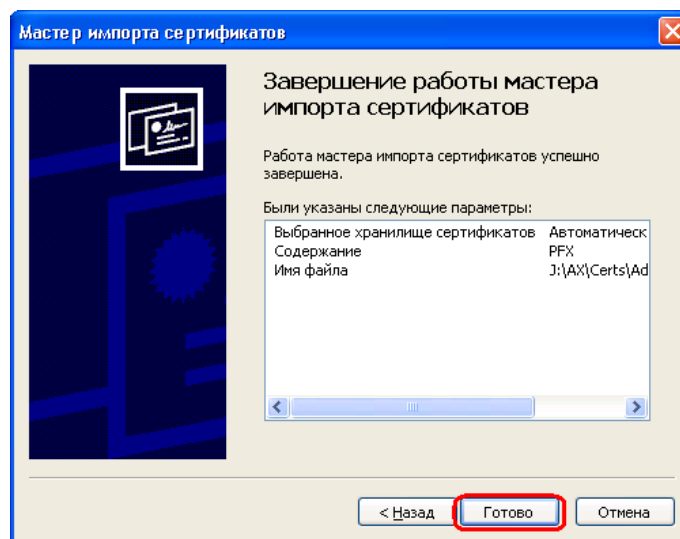


Рис. 13

Импорт сертификата администратора успешно завершён, о чем система выдаст соответствующее сообщение. Посмотреть установленный сертификат администратора можно так же, как и сертификат организации, с помощью браузера Internet Explorer.

### 3.4.9. Запуск системы удаленного администрирования.

Удаленный доступ к интерфейсу конфигурирования ПАК «СБ» осуществляется средствами веб-браузера, поддерживающего элементы ActiveX. Рекомендуемыми уровнями безопасности для зон Интернета являются настройки «по умолчанию». В настройках веб-браузера необходимо разрешить выполнение сценариев ActiveX, являющихся безопасными и подписанными доверенным центром сертификации.

При попытке соединения с сервером ПАК «СБ» веб-браузер (по умолчанию Internet Explorer) предложит выбрать сертификат, который будет предъявлен серверу для аутентификации (рис. 14). Из списка необходимо выбрать сертификат, установленный в пункте 3.4.2. данной инструкции, т.е. сертификат администратора, и нажать на кнопку «ОК».

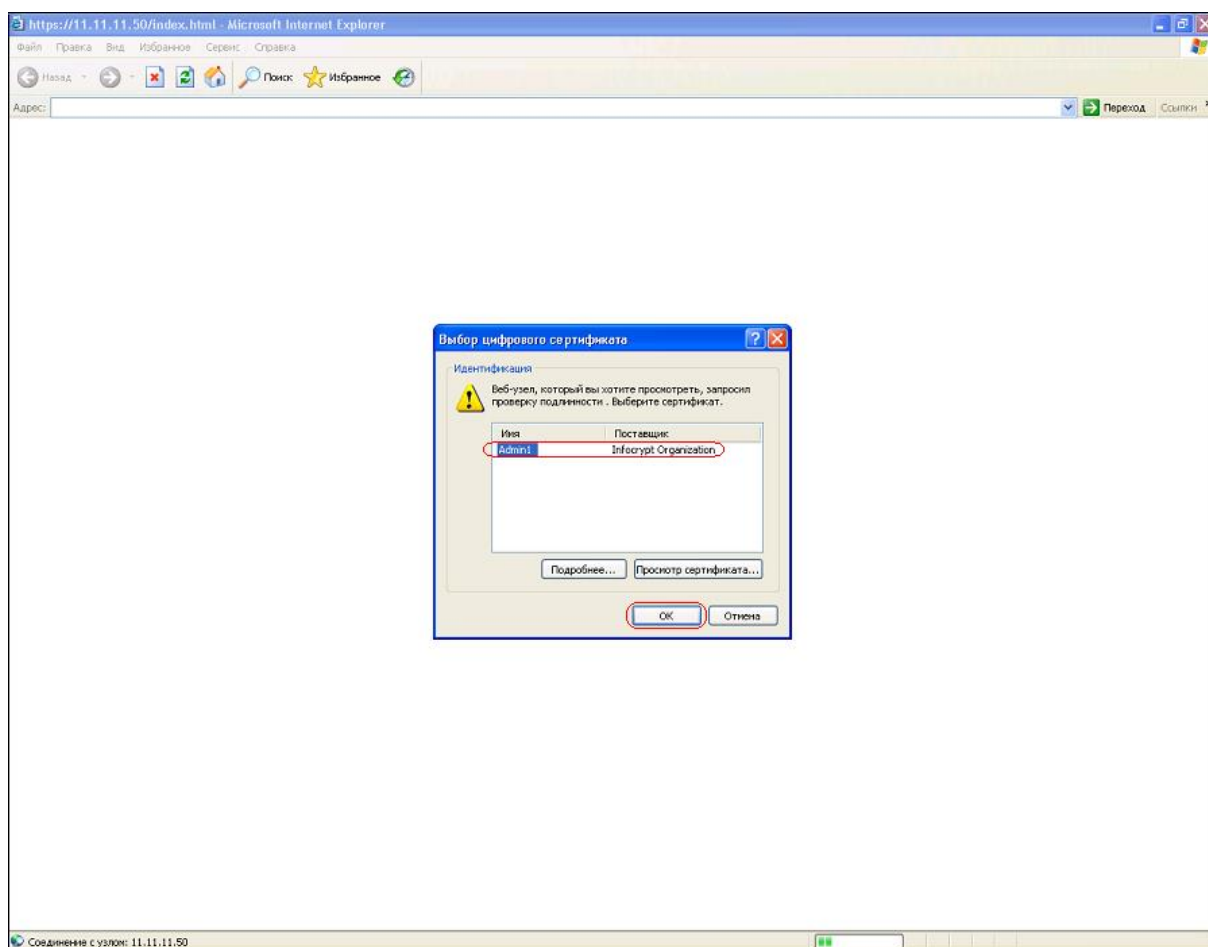


Рис. 14. Выбор сертификата удаленного администратора

После успешного соединения с ПАК «СБ» администратор обязан проверить отпечаток предъявленного ему сертификата сервера, сравнив его с тем, который был ему предоставлен при создании его собственного сертификата (сертификата администратора). Это можно сделать, щелкнув по значку замка в правой части нижней строки состояния Internet Explorer, а затем выбрав пункт «Отпечаток» на закладке «Состав» в появившемся окне.

### 3.4.10. Удаленная загрузка ключей шифрования и подписи.

Для выполнения операций загрузки ключей шифрования или подписи при первом запуске потребуется установить ActiveX компонент. Веб-браузер предложит сделать это примерно таким образом (рис. 15):

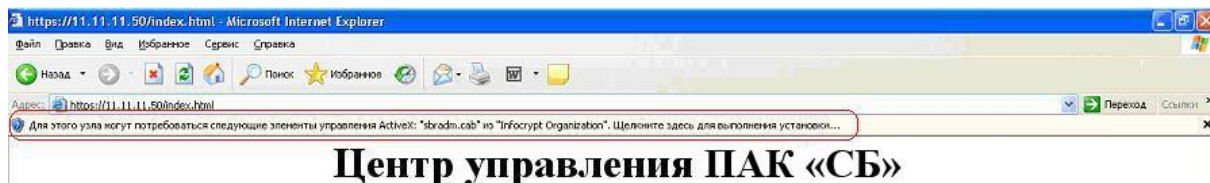


Рис. 15. Установка ActiveX компонента

После согласия на установку система выведет окно предупреждения системы безопасности. Здесь можно получить информацию как о самом компоненте, щелкнув по его наименованию, так и о сертификате, которым он подписан, щелкнув по ссылке на издателя.

Нажмите на кнопку «Установить».

Для выполнения операции шифрования также необходим файл с открытым ключом сервера **Server.pkb**. Этот файл администратор получает при снятии своих ключевых данных на USB-совместимый носитель. Файл **Server.pkb** нужно поместить в каталог установки ActiveX компонента (по умолчанию это каталог «%Системный диск%\Program Files\Infocrypt\ASDG»).

## 4. КОНФИГУРИРОВАНИЕ

### 4.1. Управление сетевыми ресурсами

Для того, чтобы конфигурировать ПАК «СБ» с удаленного рабочего места, необходимо предварительно настроить систему безопасности удаленного ПК для корректной аутентификации при установлении соединения с сервером ПАК «СБ» (см. 3.4.).

Удаленный доступ к интерфейсу конфигурирования ПАК «СБ» осуществляется средствами веб-браузера. Для этого при помощи браузера нужно перейти на страницу с URL вида «https://<сетевое имя ПАК «СБ»>/» (рис. 15).



Рис. 15. Веб-интерфейс конфигурирования ПАК «СБ»

Веб-интерфейс конфигурирования и управления предоставляет нижеперечисленные возможности по определению задач и графика обработки данных средствами ПАК «СБ».

Для просмотра списка существующих сетевых ресурсов нужно выбрать пункт меню (колонка слева) «Ресурсы». В поле по центру будет отображена таблица, строки которой описывают ресурсы, а столбцы – параметры данных ресурсов (рис. 16).

## Центр управления ПАК «СБ»

paksb-test , v.3.15.6 , 11.11.11.7104

## Параметры

- [Ресурсы](#)
- [Задачи](#)
- [Ключи шифрования](#)
- [Открытые ключи проверки подписи](#)

Управление  
конфигурацией

- [Активировать конфигурацию](#)
- [Отменить изменения конфигурации](#)
- [Сохранить копию конфигурации](#)
- [Восстановить конфигурацию](#)

## Получение ключевых данных

- [Выгрузка открытого ключа ЭЦП  
ПАК «СБ»](#)
- [Управление задачами к сервером](#)

[Журнал](#)  
[Монитор](#)  
[Обновления](#)  
[Файлы для загрузки](#)

## Список ресурсов

Имя	URL	Учетная запись	Транспорт	Таймаут	Валидность
Добавить новый					
Применить шаблон					

Рис. 16. Веб-интерфейс: таблица ресурсов

### 4.1.1. Добавление нового ресурса

Чтобы добавить к списку новый сетевой ресурс, нужно нажать на кнопку «Добавить новый», которая находится под таблицей с параметрами ресурсов.

Откроется страница добавления ресурса (рис. 17):

Рис. 17. Веб-интерфейс: добавление нового ресурса

Нужно определить параметры нового ресурса, заполнив поля формы, и нажать на кнопку «Сохранить» для подтверждения или «Отменить» для отмены и возврата к списку ресурсов.

*Пример:* описание cifs-ресурса на Windows-сервере.

Рис. 18. Пример: cifs-ресурс на Windows-сервере


Нужно указать полный путь к директории с настроенным общим доступом, выбрать «cifs» в меню транспортов, указать имя пользователя и пароль для доступа



(рис. 18). Имя ресурса может быть произвольным, оно будет использовано в таблице ресурсов и таблице задач для обозначения данного сетевого ресурса.


Аналогично задаются nfs-ресурсы и ftp-ресурсы (при этом указываются соответствующие транспорты).

#### **4.1.2. Удаление ресурса**

Чтобы удалить ресурс из списка ресурсов, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ресурсов.

Удаление ресурса невозможно, если он используется какой-либо задачей; конфигуратор выдаст сообщение об ошибке.

### 4.1.3. Редактирование ресурса

Чтобы изменить параметры существующего ресурса, нужно нажать на кнопку с пиктограммой  (слева от соответствующей строки в таблице ресурсов). На экране появится страница с параметрами ресурса, которые можно изменять.

По завершении редактирования нужно нажать на кнопку «Сохранить» для подтверждения изменений или на кнопку «Отменить» для отмены.

### 4.1.4. Создание копии ресурса

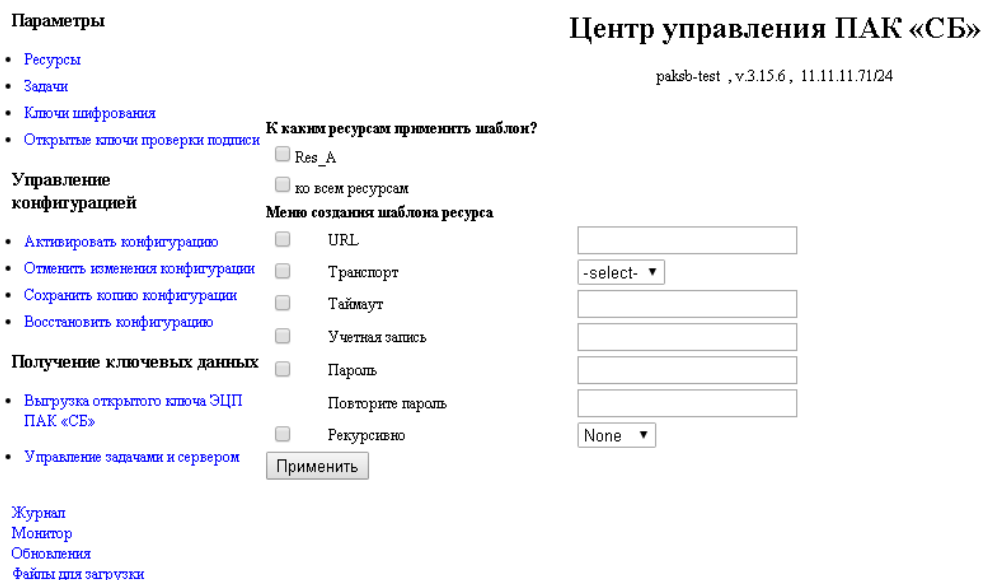
Чтобы дублировать сетевой ресурс, нужно нажать на кнопку с пиктограммой, расположенную слева от соответствующей строки в таблице ресурсов. На экране появится страница с параметрами ресурса-копии, которые можно изменять. Изначально параметры ресурса-копии совпадают с параметрами исходного ресурса.

По завершении определения параметров ресурса-копии нужно нажать на кнопку «Сохранить», чтобы добавить ресурс к списку ресурсов, или на кнопку «Отменить» для отмены создания копии.

### 4.1.5. Применение шаблона к описанию ресурсов

Предусмотрена возможность изменять параметры одного или нескольких ресурсов согласно некоторому шаблону.

Для этого нужно нажать на кнопку «Применить шаблон», в появившемся меню отметить те параметры, которые планируется изменить, ввести шаблонные значения в поля формы и выбрать ресурсы, к которым будет применен шаблон (рис. 19).



Параметры

- Ресурсы
- Задачи
- Ключи шифрования
- Открытые ключи проверки подписи

Управление конфигурацией

- Активировать конфигурацию
- Отменить изменения конфигурации
- Сохранить копию конфигурации
- Восстановить конфигурацию

Получение ключевых данных

- Выгрузка открытого ключа ЭЦП ПАК «СБ»
- Управление задачами и сервером

Журнал  
Монитор  
Обновления  
Файлы для загрузки

Центр управления ПАК «СБ»

paksb-test, v.3.15.6, 11.11.11.71/24

К каким ресурсам применить шаблон?

Res\_A

ко всем ресурсам

Меню создания шаблона ресурса

URL

Транспорт

Таймаут

Учетная запись

Пароль

Повторите пароль

Рекурсивно

-select- ▼


None ▼


Рис. 19. Веб-интерфейс: применение шаблона к описанию сетевых ресурсов


После чего нужно нажать на кнопку «Применить» для сохранения изменений и на кнопку «Отменить» для отмены и возврата к таблице ресурсов.

#### 4.1.6. Проверка валидности описания ресурса и доступности ресурса



Пиктограмма в графе «Валидность» в таблице ресурсов отражает корректность описания ресурса.

Если какие-либо параметры ресурса заданы некорректно, то в графе «Валидность» таблицы ресурсов в соответствующей строке отображается кнопка с пиктограммой ; нажав на нее, можно получить список нуждающихся в исправлении параметров ресурса.

Если ресурс задан корректно, то в графе «Валидность» отображается пиктограмма .

В таблице ресурсов слева от каждой строки расположена кнопка с пиктограммой . Нажав на нее, можно получить информацию о доступности сетевого ресурса в данный момент.

Также можно получить информацию о доступности всех сетевых ресурсов в данный момент, для этого нужно нажать на кнопку «Доступность», расположенную под таблицей описания ресурсов.

Доступные ресурсы будут помечены пиктограммой  в графе «Валидность», недоступные – пиктограммой .

## 4.2. Управление ключами шифрования

Для просмотра списка установленных ключей шифрования необходимо выбрать пункт меню (колонка слева) «Ключи шифрования». В поле по центру будет отображена таблица, строки которой описывают ключи шифрования, а столбцы – параметры данных ключей (рис. 19).

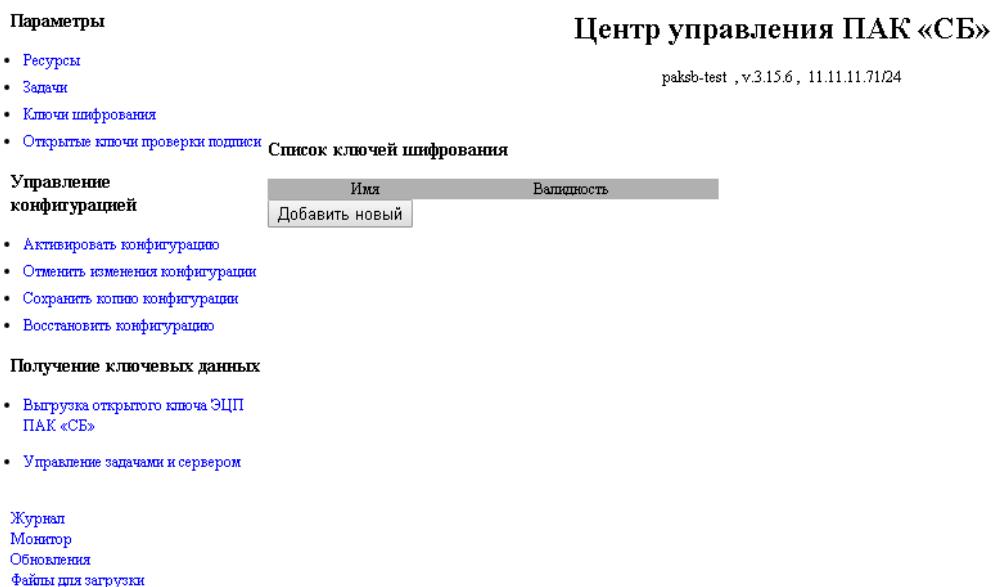


Рис. 19. Веб-интерфейс: список ключей шифрования

### 4.2.1. Добавление нового ключа шифрования


Чтобы установить новый ключ шифрования, нужно нажать на кнопку «Добавить», которая отображается под таблицей с параметрами ключей.

При добавлении нужно определить имя ключа (оно будет отображаться в таблице ключей шифрования, а также использоваться при определении параметров задачи), нажать на кнопку «Сохранить» и выбрать файл ключа. На экране появится сообщение, требующее предъявить ключ удаленного администратора.

Нужно приложить ТМ-носитель с ключом удаленного администратора (ТМ-носитель с наклейкой «АДМ») к считывателю.


Чтобы отменить операцию и вернуться к таблице ключей шифрования, нужно нажать на кнопку «Отменить».

### 4.2.2. Удаление ключа шифрования

Чтобы удалить ключ шифрования, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ключей шифрования.


Удаление ключа невозможно, если он используется какой-либо задачей; конфигуратор выдаст сообщение об ошибке.

### 4.2.3. Редактирование ключа шифрования

Чтобы изменить имя ключа или указать новый файл ключа шифрования, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ключей шифрования. Откроется страница, позволяющая изменить параметры ключа шифрования.

По завершении редактирования необходимо нажать на кнопку «Сохранить», выбрать файл ключа и в ответ на просьбу предъявить ключ администратора приложить к считывателю соответствующий ТМ-носитель. Для отмены и возврата к таблице ключей шифрования нужно нажать на кнопку «Отменить».


### 4.2.4. Создание копии ключа шифрования


Чтобы дублировать ключ шифрования, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки таблицы ключей шифрования. Откроется страница с параметрами ключа-копии, которые можно изменять. Изначально параметры ключа-копии совпадают с параметрами исходного ключа.

По завершении определения параметров ключа-копии необходимо нажать на кнопку «Сохранить», выбрать файл ключа и в ответ на просьбу предъявить ключ администратора приложить к считывателю соответствующий ТМ-носитель. Для отмены и возврата к таблице ключей шифрования нужно нажать на кнопку «Отменить».

### 4.2.5. Проверка корректности описания ключа

Пиктограмма в графе «Валидность» в таблице ключей шифрования отражает корректность описания ключа шифрования.

Если параметры ключа заданы некорректно, то в соответствующей строке в графе «Валидность» таблицы ключей шифрования отображается кнопка с пиктограммой , нажав на которую можно получить список нуждающихся в исправлении параметров ключа.

Если ключ шифрования задан корректно, то в графе «Валидность» отображается пиктограмма .

### 4.3. Управление ключами проверки подписи

Для просмотра списка установленных ключей проверки подписи необходимо выбрать пункт меню (колонка слева) «Открытые ключи проверки подписи». В поле по центру будет отображена таблица, строки которой описывают ключи проверки подписи, а столбцы – параметры данных ключей (рис. 20).

**Параметры**

- Ресурсы
- Задачи
- Ключи шифрования
- Открытые ключи проверки подписи

**Управление конфигурацией**

- Активировать конфигурацию
- Отменить изменения конфигурации
- Сохранить копию конфигурации
- Восстановить конфигурацию

**Получение ключевых данных**

- Выгрузка открытого ключа ЭЦП ПАК «СБ»
- Управление задачами и сервером

Журнал  
Монитор  
Обновления  
Файлы для загрузки

**Центр управления ПАК «СБ»**  
paksb-test , v.3.15.6 , 11.11.11.71/24

**Список открытых ключей проверки подписи**

Имя	Валидность
Добавить новый	

Рис. 20. Веб-интерфейс: список открытых ключей проверки подписи

#### 4.3.1. Добавление нового ключа проверки подписи


Чтобы установить новый ключ проверки подписи, нужно нажать на кнопку «Добавить», которая отображается под таблицей с параметрами ключей. На экране появится форма добавления нового ключа шифрования.

Нужно определить параметры нового ключа проверки подписи, заполнив поля формы (указать имя ключа, выбрать из существующих (или создать новую) базу открытых ключей, куда будет помещен этот ключ), и нажать на кнопку «Сохранить». После этого нужно выбрать файл ключа или базы открытых ключей.

На экране появится сообщение, требующее предъявить ключ удаленного администратора. Необходимо приложить ТМ-носитель с ключом удаленного администратора (ТМ-носитель с наклейкой «АДМ») к считывателю.


Для отмены и возврата к списку установленных ключей нажмите на кнопку «Отменить».

#### 4.3.2. Удаление ключа проверки подписи

Чтобы удалить ключ проверки подписи, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ключей проверки подписи.


Удаление ключа невозможно, если он используется какой-либо задачей; конфигуратор выдаст сообщение об ошибке.

#### **4.3.3. Редактирование ключа проверки подписи**

Чтобы изменить параметры ключа проверки подписи, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ключей проверки подписи. На экране отобразится страница, предоставляющая возможность изменить имя ключа и выбрать базу открытых ключей для сохранения ключа в данную базу.

По завершении редактирования нужно нажать на кнопку «Сохранить», и в ответ на просьбу предъявить ключ администратора приложить к считывателю соответствующий ТМ-носитель, а затем выбрать файл ключа (базы ключей). Для отмены и возврата к таблице ключей проверки подписи нужно нажать на кнопку «Отменить».


#### **4.3.4. Создание копии ключа проверки подписи**


Чтобы дублировать ключ проверки подписи, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице ключей проверки подписи. На экране появится страница с параметрами ключа-копии, которые можно изменять. Изначально параметры ключа-копии совпадают с параметрами исходного ключа.

По завершении определения параметров ключа-копии нужно нажать на кнопку «Сохранить», и в ответ на просьбу предъявить ключ администратора приложить к считывателю соответствующий ТМ-носитель, а затем выбрать файл ключа (базы ключей). Для отмены и возврата к таблице ключей проверки подписи нужно нажать на кнопку «Отменить».

#### **4.3.5. Проверка корректности описания ключа**

Пиктограмма в графе «Валидность» в таблице ключей проверки подписи отражает корректность описания ключа шифрования.

Если параметры ключа заданы некорректно, то в соответствующей строке в графе «Валидность» таблицы ключей проверки подписи отображается кнопка с пиктограммой , нажав на которую можно получить список нуждающихся в исправлении параметров ключа.

Если ключ проверки подписи задан корректно, то в графе «Валидность» отображается пиктограмма .



## 4.4. Управление задачами обработки

Для просмотра списка существующих задач обработки данных выберите пункт меню (колонка слева) «Задачи».

В поле по центру будет отображена таблица, строки которой описывают задачи, а столбцы – параметры данных задач (рис. 21).

Параметры

- Ресурсы
- Задачи
- Ключи шифрования
- Открытые ключи проверки подписи

Управление конфигурацией

- Активировать конфигурацию
- Отменить изменения конфигурации
- Сохранить копию конфигурации
- Восстановить конфигурацию

Получение ключевых данных

- Выгрузка открытого ключа ЭЦП ПАК «СБ»
- Управление задачами и сервером

Журнал  
Монитор  
Обновления  
Файлы для загрузки

Центр управления ПАК «СБ»  
paksb-test , v.3.15.6 , 11.11.11.71/24

Список задач

Выделить все      Снять выделение

id	Имя	Ресурс источник	Ресурс приемник	Расписание	Операции и ключи к ним	Валидность
Сохранить						
Добавить						
Применить шаблон						

Рис. 21. Веб-интерфейс: таблица задач обработки

### 4.4.1. Добавление новой задачи

Чтобы добавить новую задачу обработки, нужно нажать на кнопку «Добавить», расположенную под таблицей с параметрами задач. Откроется страница добавления новой задачи (рис. 22).

Определите параметры задачи, заполнив поля формы.

Операцию и соответствующий ей ключ выберите из выпадающего списка, затем нажмите на ссылку «Add» справа. Проведите эти действия для всех необходимых операций.

Нажмите на кнопку «Сохранить» для подтверждения и добавления задачи в список, или «Отменить» для отмены и возврата к таблице задач.

### Центр управления ПАК «СБ»

pak8b-test , v3.15.6 , 11.11.11.7124

**Параметры**

- Ресурсы
- Задачи
- Ключи шифрования
- Открыть» ключи проверки подписей

**Управление конфигурацией**

- Активировать конфигурацию
- Отменить изменения конфигурации
- Сохранить копию конфигурации
- Восстановить конфигурацию

**Получение ключевых данных**

- Выгрузить открытый ключ ЭЦП ПАК «СБ»
- Управление запчаами и сервером

Имя задачи:  Включить при активации

Ресурс источник:  Вложенный путь на источнике:  Маска на источнике:

Ресурс приемник:  Вложенный путь на приемнике:  Маска на приемнике:

Ресурс архив:  Вложенный путь на архиве:  Маска на архиве:

Ресурс ошибок:  Вложенный путь на ошибках:  Маска на ошибках:

Приоритет:  Рекурсивно:  Уровень рекурсии:

Детализация журнала:  Детализация статистики:  Время ожидания:

Путь на приемнике:  Тип сортировки:  Тип синхронизации:

Макс размер файла [MB]:  Макс размер в сгруппе [MB]:  Макс кол-во файлов:

Удалить файлы при перезаписи:

Операции и ключи к ним

повисг	sign key	<input type="button" value="↺"/>	<input type="button" value="↻"/>	<input type="button" value="✖"/>
повисг	sign key	<input type="button" value="Добавить"/>		

Минуты:  Каждый месяц:  Каждый час:  Каждый день:  Каждый месяц:  Каждый день:

Выбрать:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:

Выбрать:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:

Выбрать:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:

Выбрать:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:

Выбрать:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:  Выберите:

Количество запусков в минуту:

Журнал  
Монитор  
Обновления  
Файлы для загрузки

Рис.22. Веб-интерфейс: добавление новой задачи

Допускается не указывать ресурс-архив и ресурс ошибок, оставляя пустыми соответствующие поля. В этом случае архивация данных и сохранение результатов неудачных операций производиться не будет.

Чтобы изменить порядок операций, воспользуйтесь кнопками с пиктограммами и , расположенными справа от каждой добавленной операции. Чтобы исключить операцию из списка, нажмите на кнопку с пиктограммой в соответствующей строке.

В качестве значения параметра «Рекурсивно» необходимо выбрать тип алгоритма рекурсивной обработки вложенной структуры директорий источника. Доступны значения None, Folder, Tree.

В случае выбора первого значения рекурсивная обработка исключается. Будут обработаны файлы на первом уровне вложенности.

В случае выбора значения Folder будет выполнена обычная рекурсивная обработка до достижения указанного дополнительно уровня вложенности.

В случае выбора значения Tree применяется отдельный алгоритм рекурсивной обработки вложенных поддиректорий ПЕРВОГО уровня вложенности с использованием дополнительного параметра «Вложенный путь», структура которых рассматривается на следующем примере.

Хоста/

ресурс\_хоста\_A/

поддиректория\_1/

IN/


OUT/

```
поддиректория_2/  
    IN/  
    OUT/  
.....  
поддиректория_N/  
    IN/  
    OUT/  
  
ХостБ/  
    ресурс_хоста_Б/  
        поддиректория_1/  
            IN/  
            OUT/  
        поддиректория_2/  
            IN/  
            OUT/  
.....  
        поддиректория_N/  
            IN/  
            OUT/
```


Эту структуру обработают 2 задачи.

1. Первая задача - из "хостА/ресурс\_хоста\_А" в "хостБ/ресурс\_хоста\_Б" с типом рекурсии "Tree", и Вложенный путь на источнике "OUT", на приемнике "IN".
2. Вторая задача - из "хостБ/ресурс\_хоста\_Б" в "хостА/ресурс\_хоста\_А" с типом рекурсии "Tree", и Вложенный путь на источнике "OUT", на приемнике "IN".

#### 4.4.2. Удаление задачи

Чтобы удалить задачу из списка задач обработки, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице с параметрами задач.

#### 4.4.3. Редактирование задачи

Чтобы изменить параметры задачи, нужно нажать на кнопку с пиктограммой , расположенную слева от соответствующей строки в таблице с параметрами задач. На экране появится страница с параметрами задачи, которые можно изменять.

Нажмите на кнопку «Сохранить» для подтверждения изменений или на кнопку «Отменить» для отмены.

#### 4.4.4. Создание копии задачи

Чтобы дублировать некоторую задачу, нужно нажать на кнопку с пиктограммой (слева от соответствующей строки в таблице с параметрами задач).

На экране появится страница с параметрами новой задачи, которые можно изменять. Изначально параметры задачи-копии совпадают с параметрами исходной задачи.

Нажмите на кнопку «Сохранить» для добавления задачи-копии к списку задач, или на кнопку «Отменить» для отмены создания копии.

#### 4.4.5. Применение шаблона к описанию задач

Предусмотрена возможность изменять параметры одной или нескольких задач согласно некоторому шаблону.

Для этого нужно нажать на кнопку «Применить шаблон» (расположенную под таблицей с параметрами задач), в появившемся меню отметить флажками те параметры, которые планируется изменить, ввести в поля формы шаблонные значения и отметить флажком задачи, к которым будет применен шаблон.

После этого нужно нажать на кнопку «Применить» для применения шаблона к выбранным задачам, или на кнопку «Отменить» для отмены и возврата к таблице задач.

#### 4.4.6. Выбор задач для включения в рабочую конфигурацию

По окончании редактирования списка задач необходимо выбрать те, которые планируется включить в рабочую конфигурацию ПАК «СБ».

Те задачи, которые должны выполняться ПАК «СБ» в данной конфигурации, необходимо отметить флажком (слева от каждой строки в таблице задач). После активации конфигурации (см. 4.6) будут выполняться они и только они.

Неотмеченные задачи не будут включены в рабочую конфигурацию, но будут доступны для дальнейшего редактирования и последующего включения.

#### **4.5. Активация конфигурации**

Все изменения конфигурации вступают в силу только после ее активации. По завершении правок конфигурации (редактирования или добавления новых элементов, конвертации ini-файлов) необходимо активировать новые параметры. Для этого следует выбрать пункт меню «Активировать конфигурацию» и подтвердить намерения нажатием на кнопку «Активировать», появившуюся в центральной части экрана.

При активации конфигурации будут учтены только те задачи, которые отмечены флажком в таблице задач (см. 4.4.6).

Если конфигурация содержит невалидные ресурсы (ключи, задачи), то активация конфигурации произведена не будет. Необходимо исправить параметры невалидных ресурсов, ключей или задач, или исключить невалидные задачи из рабочей конфигурации (сняв соответствующие флажки в таблице задач).

#### 4.5.1. Отмена изменений

Чтобы вернуться к последней активированной версии, нужно выбрать пункт меню «Отменить изменения конфигурации».

Подтвердите намерения нажатием на кнопку «Отменить», появившуюся в центральной части экрана.

Все изменения, внесенные с момента последней активации, будут аннулированы. В таблицах будут отображаться параметры последней активированной версии конфигурации. Они также будут доступны для редактирования.

Обратите внимание, что задачи, которые не были отмечены флажком при активации конфигурации, в активную конфигурацию не включаются, и поэтому после отмены изменений они безвозвратно исчезнут из таблицы задач.

#### 4.6. Создание резервной копии конфигурации

Предусмотрена возможность сохранения конфигурации ПАК «СБ» для ее последующего восстановления при необходимости. Для этого нужно выбрать пункт меню веб-интерфейса удаленного администрирования «Сохранить копию конфигурации».

Загруженный файл будет содержать резервную копию параметров конфигурации – таблицы ресурсов, задач, ключей шифрования и ключей проверки подписи, файлы загруженных ключей шифрования и ключей проверки подписи.

**ВАЖНО!** Файл резервной копии конфигурации зашифрован на ключе хранения резервных копий (см. 3.2.5.3), который, в свою очередь, зашифрован на ключе офицера безопасности (см. 3.2.5.1). Если с момента сохранения копии конфигурации эти ключи были изменены, то до их восстановления **восстановление конфигурации будет невозможно.**

#### 4.7. Восстановление конфигурации

Для восстановления предварительно сохраненной копии конфигурации ПАК «СБ» нужно выбрать пункт меню веб-интерфейса удаленного администрирования «Восстановить конфигурацию».

Нужно указать файл, содержащий предварительно сохраненную копию конфигурации, и нажать на кнопку «Отправить».

Параметры восстановленной конфигурации будут доступны для просмотра и редактирования средствами веб-интерфейса удаленных администраторов.

Чтобы восстановленная конфигурация вступила в силу, нужно ее активировать. Чтобы восстановить последнюю активированную конфигурацию (на момент сохранения резервной копии), выберите пункт меню слева «Отменить изменения конфигурации» и нажмите на кнопку «Отменить». Внесите изменения, если это необходимо, и активируйте полученную конфигурацию.

Перед восстановлением конфигурации из резервной копии может потребоваться восстановление ключа хранения резервных копий, использовавшегося на момент сохранения этой резервной копии, а также ключа офицера безопасности, на котором тот был зашифрован.

Сначала для того, чтобы восстановить ключ офицера безопасности, выберите пункт меню локальной консоли управления «**Sec. officer key**», затем подпункт «**Import from the external device**», и приложите к считывателю ТМ-носитель с соответствующим ключом офицера безопасности.

Затем для восстановления ключа резервных копий выберите пункт меню локальной консоли управления «**Backup key**», затем подпункт «**Import from the external device**», и приложите к считывателю ТМ-носитель с соответствующим ключом хранения резервных копий.

В целом, нет необходимости восстанавливать ключ офицера безопасности (*Коб*), если все изменения этого ключа сопровождалась выгрузкой зашифрованного на новом *Коб* ключа хранения резервных копий (см. 3.2.5.3). Однако, все ключи шифрования и ключи проверки подписи шифруются на *Коб*, и в том случае, если *Коб* изменился с момента сохранения резервной копии, понадобится либо заново загрузить файлы ключей после восстановления конфигурации (отредактировав соответствующие записи в таблицах ключей, см. 4.2.3, 4.3.3), либо предварительно восстановить тот *Коб*, который использовался на момент сохранения, и ключ резервного копирования, ему соответствующий (зашифрованный на этом *Коб*).

#### **4.8. Выгрузка открытого ключа ЭЦП**

В задачи ПАК «СБ» по обработке файлового ресурса может входить операция формирования электронной цифровой подписи (ЭЦП). Для проверки сформированной ПАК «СБ» ЭЦП требуется открытый ключ ЭЦП ПАК «СБ». Этот ключ можно получить средствами web-интерфейса конфигулятора.

Выберите пункт меню слева «Выгрузка открытого ключа ЭЦП ПАК „СБ“», чтобы загрузить файл ключа.

Полученный файл можно установить в качестве ключа проверки подписи для операции проверки ЭЦП в задачах ПАК «СБ» (см. 4.3).



#### **4.9. Режим параллельной обработки**

Возможно организовать параллельную обработку файловых ресурсов SMB средствами нескольких ПАКСБ, которые будут к этим ресурсам подключаться одновременно. Для этого в ПО ПАКСБ встроена поддержка совместной работы на ресурсах такого типа с другими ПАКСБ. Поддержка заключается в интеграции в конвейер операций по обработке файлов на ресурсе действий по проверке «занятости» файлов, «занятию» файлов и их «освобождению» по результатам обработки.

Алгоритм совместной работы ПАКСБ по общим файловым ресурсам типа SMB включает ряд шагов, а именно: при подключении к ресурсу осуществляется его просмотр и составление перечня файлов для обработки. В перечень включаются те файлы, которые еще не «заняты» обработкой, которая началась ранее. Если файл еще не «занят», то он «занимается», т.е. принимается в обработку. Для такого файла создается дополнительный файл, имя которого формируется, как имя исходного файла + «.ЛОК». Такой ЛОК-файл снабжается соответствующим признаком, защищающим его от модификации процессом, отличным от создавшего его процесса-обработчика. Таким образом, когда «занятый» исходный файл проверяется на «занятость» другим процессом-обработчиком, фиксируется наличие ЛОК-файла, который этому процессу не удастся модифицировать. Обнаруженный в соответствии с таким признаком «занятости» файл не включается в обработку при подключении и просмотре ресурса.

Таким образом, организация режима параллельной обработки средствами нескольких ПАКСБ не требует каких-либо дополнительных действий при задании конфигурации обработки.

## 5. МОНИТОРИНГ

### 5.1. Просмотр системного журнала

Сжатая копия системного журнала может быть получена удаленным администратором при выборе пункта меню веб-интерфейса «Журнал» (рис. 23).

Предоставляется возможность получить выборку записей за некоторый период времени, а также изменить длительность хранения старых записей.

Для получения выборки нужно установить дату начала выборки и дату окончания, а затем нажать на кнопку «Сформировать». Будет сформирован список файлов, содержащих записи за выбранный период времени. Чтобы загрузить файлы отчетов, нажмите на появившуюся ссылку «Загрузить лог». Файлы будут загружены одним архивом.

Чтобы изменить длительность хранения старых записей, введите количество дней в соответствующее поле. По умолчанию записи хранятся 10 дней.

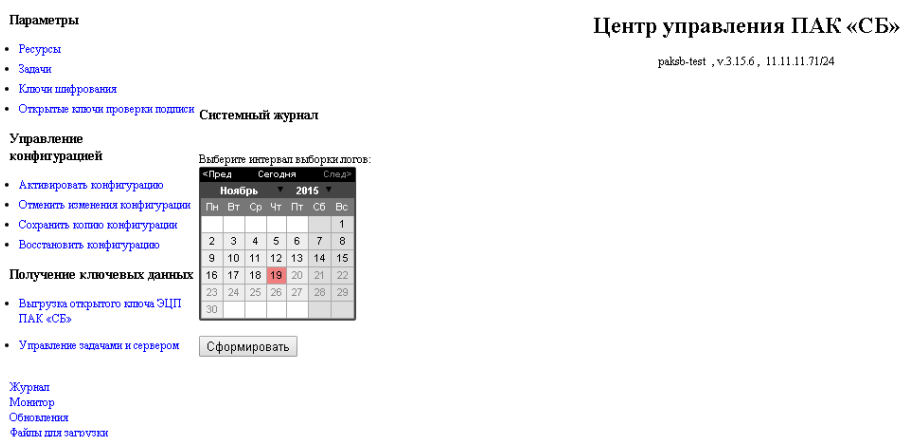


Рис. 23. Веб-интерфейс: формирование выборки записей системного журнала

### 5.2. Просмотр текущего состояния системы

Перечень задач, которые обрабатываются ПАК «СБ» в данный момент времени, можно получить как через локальную консоль управления, так и через веб-интерфейс удаленного администрирования, выбрав пункт меню «Монитор». В обоих случаях будет отображена следующая информация:

- список выполняемых задач расписания;
- количество уже обработанных файлов по данным задачам;
- доля ресурсов ЦП, которые расходуются на выполнение каждой задачи.

### 5.3. Остановка системы

Остановить ПАК «СБ» можно при помощи локальной консоли управления. Для этого нужно выбрать пункт меню «**Turn off**».

#### **5.4. Перегрузка системы**

Перезагрузить ПАК «СБ» можно при помощи локальной консоли управления. Для этого нужно выбрать пункт меню «**Reboot**».

## 6. ОБНОВЛЕНИЕ

Предусмотрена возможность автоматического обновления системы. Обновления выпускаются производителем и распространяются среди пользователей в виде зашифрованных файлов. Способ установки зависит от типа полученного обновления: файлы обновлений «**icsbupdate.bin**» устанавливаются через меню загрузки ПАК «СБ», файлы с расширением «**.upd**» – через меню веб-интерфейса.

Перед установкой обновления сохраните резервную копию конфигурации ПАК «СБ» (см. 4.7).

### 6.1. Установка обновлений через меню загрузки

Запишите полученный файл обновления (файл **icsbupdate.bin**) на USB-совместимый носитель. Перезагрузите ПАК «СБ», при загрузке выберите пункт меню «**Install update**» и следуйте инструкции на экране.

### 6.2. Установка обновлений через меню веб-интерфейса

Выберите пункт «Обновление» в меню слева. На экране появится форма загрузки обновления (рис. 24):



Рис. 24. Веб-интерфейс: загрузка обновлений

Укажите имя устанавливаемого обновления и нажмите на кнопку «Сохранить». Затем выберите файл обновления (файл с расширением «**.upd**»).

ПАК «СБ» автоматически установит загруженное обновление.

Нажмите на кнопку «Отменить», если хотите отказаться от загрузки обновления и вернуться в главное меню.

### 6.3. Возвращение к предыдущей версии

Чтобы после обновления системы вернуться к предыдущей версии ПАК «СБ», перезагрузите ПАК «СБ» и при загрузке выберите пункт меню «**Rollback last update**».

Чтобы восстановить исходные (заводские) параметры ПАК «СБ», перезагрузите ПАК «СБ» и при загрузке выберите пункт меню «**Reset factory settings**». После восстановления настроек при первом запуске может появиться предупреждение о том, что предыдущая установка завершилась неудачно. Это не является ошибкой, в диалоговом окне на вопрос о продолжении установки нужно выбрать вариант «да».

В обоих случаях отката настроек для восстановления параметров конфигурации ПАК «СБ» (параметров ресурсов, задач, и так далее) может потребоваться предварительно сохраненная резервная копия конфигурации (см. 4.7, 4.8).

## **7. АВАРИЙНЫЕ СИТУАЦИИ**

При отказе технических средств, в случае несанкционированного вмешательства в данные и в других аварийных ситуациях необходимо по возможности выполнить сбор максимального объема доступной информации о состоянии ПАК «СБ» (мониторинг), о событиях, предшествовавших моменту возникновения проблем (журнал). Эти данные необходимо предоставить в службу технической поддержки.