

ООО Фирма Инфокрипт

**ПАК Планировщик Файловых Операций (Beta)
Руководство пользователя**

Москва 2010

1 Введение	3
1.1. Область применения	3
1.2. Краткое описание возможностей	3
1.3. Уровень подготовки пользователя	4
1.4. Перечень эксплуатационной документации	4
2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ	5
2.1. Виды деятельности, функции	5
2.2. Программные и аппаратные требования к системе	7
3 ПОДГОТОВКА К РАБОТЕ	8
3.1. Состав дистрибутива	8
3.2. Запуск системы	8
3.3. Проверка работоспособности системы	13
3.4. Настройка удаленного доступа	14
4 КОНФИГУРИРОВАНИЕ	23
4.1. Управление задачами обработки	23
4.2. Управление сетевыми ресурсами	25
4.3. Управление ключами шифрования	27
4.4. Управление ключами проверки подписи	29
4.5. Конвертация конфигурационных файлов к новому формату	31
4.6. Активация конфигурации	34
4.7. Создание резервной копии конфигурации	34
4.8. Восстановление конфигурации	34
5 Мониторинг	35
5.1. Просмотр системного журнала	35
5.2. Просмотр текущего состояния системы	35
5.3. Остановка системы	35
5.4. Перезагрузка системы	35
6 Обновление	37
7 АВАРИЙНЫЕ СИТУАЦИИ	38

1 ВВЕДЕНИЕ

ПАК ПФО предназначен для обеспечения транзита защищенной информации между различными сегментами локальных сетей в соответствии с предварительно определенным графиком.

1.1. Область применения

ПФО рассчитан на применение в локальных сетях стандарта IEEE 802.3, при помощи которых необходимо выполнить межсетевую передачу данных по протоколам CIFS, SMB, NFS, POP3, FTP.

1.2. Краткое описание возможностей

ПФО 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
 - контроль целостности системы
 - 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

- выдача 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
8. автоматизированная проверка целостности носителей

1.3. Уровень подготовки пользователя

1.4. Перечень эксплуатационной документации

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Виды деятельности, функции

ПАК ПФО - это IBM-совместимый компьютер с одним или несколькими сетевыми интерфейсами. В качестве клиента он может подключаться к различным сетевым ресурсам (протоколы SMB, NFS) и сервисам (протоколы FTP, POP3, IMAP, ICQ).

Основная задача ПФО 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, ПФО играет роль многофункционального файлового и почтового шлюза.

Задача ПФО 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.



Рис.1. Структура полей объекта типа «Задача»

Ресурс определяется следующими параметрами:

- имя ресурса,
- URL,
- сетевой транспорт,
- имя пользователя для подключения,
- пароль для подключения,
- таймаут подключения,
- флаг рекурсивной обработки.

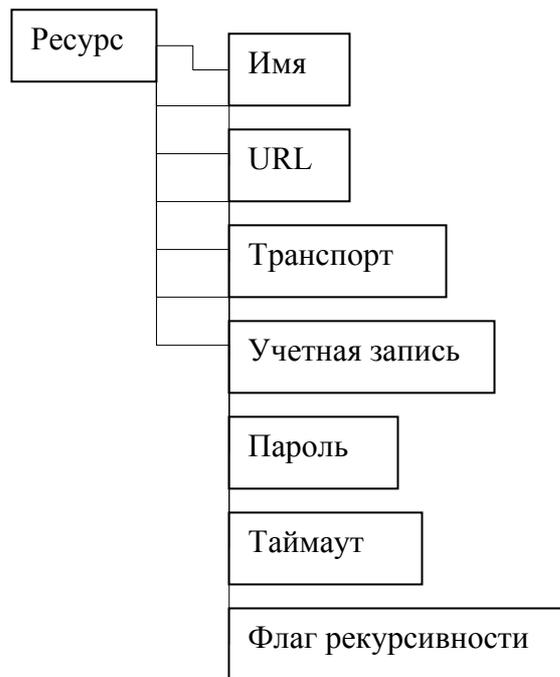


Рис.2. Структура полей объекта типа «Ресурс»

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 ПФО необходимы:

- одно или несколько подключений к Ethernet
- наличие на доступных по сети узлах открытых для удаленного доступа ресурсов SMB, NFS или серверов POP3, FTP.
- набор файлов, содержащих конфигурационные параметры системы.

3 ПОДГОТОВКА К РАБОТЕ

3.1. Состав дистрибутива

Аппаратное обеспечение ПАК ПФО составляет системный блок с установленными адаптером Аккорд АМДЗ, адаптерами сетевых интерфейсов, адаптером видеоинтерфейса.

Программное обеспечение ПАК ПФО представляет собой установленную ОС Linux, ПО ПФО, средства ключевания.

3.2. Запуск системы

3.2.1. Создание сертификата организации

Сертификат организации является основным сертификатом, используемым в системе удаленного доступа к серверу ПФО. 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 ПФО.

Выработка сертификата организации осуществляется при первом запуске сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Organization cert**», заполнить необходимые информационные поля и далее следовать инструкции.

3.2.2. Замена сертификата организации

Процедура замены сертификата организации может происходить планово или в результате каких-либо непредвиденных обстоятельств (срочная замена).

Действия при плановой замене:

1. За месяц до истечения срока действия старого сертификата всем администраторам сервера ПФО направляется уведомление о необходимости сменить сертификат организации. Уведомление размещается на основной странице web интерфейса сервера, а также, опционально, может быть направлено по электронной почте администраторам.
2. Один из администраторов сервера ПФО создает штатными средствами новый сертификат организации.
3. Система подписывает существующий запрос на сертификат сервера ПФО (либо созданный ранее новый запрос, если предполагается также замена сертификата сервера ПФО) новым сертификатом организации, тем самым создавая новый сертификат сервера ПФО, но пока не заменяет им старый. Также сохраняется отпечаток нового сертификата сервера ПФО.
4. Администратор создает штатными средствами свой новый сертификат для удаленного доступа к серверу ПФО, 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 сервере ПФО 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 ПФО по сертификатам администраторов, подписанным старым сертификатом организации, будет прекращен. Пользоваться необходимо новыми сертификатами. Проверку отпечатка сертификата сервера также надо 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.

3.2.3. Создание сертификата сервера

Сертификат применяется в системе удаленного доступа к серверу ПФО. 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 сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Server cert**», заполнить необходимые информационные поля и далее следовать инструкции.

3.2.4. Создание сертификата удаленного администратора

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

Выработка сертификата удаленного администратора осуществляется при первом запуске сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Remote admin cert**», заполнить необходимые информационные поля и далее следовать инструкции.

3.2.5. Выработка ключевых данных

2.1.6.2. 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), вырабатывается в двух экземплярах (на двух ТМ). Основная копия отдается на хранение офицеру безопасности. Резервная копия должна храниться в защищенном месте с ограниченным доступом (меры предосторожности определяются внутренним регламентом организации).

Выработка Коб осуществляется при первом запуске сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Sec. officer key**» и далее следовать инструкции на экране.

2.2.6.2. 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 сервера ПФО требуется предъявить Коб, на котором расшифруется Кз, на котором, в свою очередь, расшифруется защищенная область диска.

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

2.3.6.2. Выработка ключа хранения резервных копий

Ключ хранения резервных копий (Кв) – ключ, на котором шифруются резервные копии настроек сервера ПФО. Вырабатывается в двух экземплярах. Основная копия хранится в зашифрованном на Коб виде на жестком диске. Резервная копия ключа хранится на ТМ в месте с ограниченным доступом (определяется внутренним регламентом организации). Если при восстановлении данных из резервной копии Кв оказывается недоступен с жесткого диска, то его можно предъявить с ТМ по соответствующему запросу.

Выработка Кв осуществляется при первом запуске сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Backup key**» и далее следовать инструкции на экране.

2.4.6.2. Выработка ключа удаленного администратора

Ключ удаленного администратора (Кк) – ключ для шифрования и подписи данных перед отправкой их с удаленного рабочего места на сервер ПФО.

Выработка Кк осуществляется при первом запуске сервера ПФО. Для этого необходимо в меню конфигуратора выбрать пункт «**Remote adm. key**» и далее следовать инструкции на экране.

2.5.6.2. Выработка ключа проверки целостности

Ключ проверки целостности (Ки) – ключ, на котором подписывается список файлов, контролируемых при загрузке системы.

3.2.6. Последовательность действий при загрузке ПФО

Содержание процесса загрузки ПФО различается для случаев первого запуска и всех последующих.

2.6.6.2. Первый запуск системы

а) на данный момент система не содержит конфигурационных данных, кроме настроенного комплекса доверенной загрузки ОС. В ответ на приглашение необходимо приложить к считывателю ТМ-носитель с ключом офицера безопасности для продолжения загрузки системы.

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



Рис. 3. Окно мониторинга локальной консоли управления

В меню доступны пункты:

- Login & configure – настройка параметров системы,
- Reboot – перезагрузка системы,
- Turn off – выключение системы.

в) в случае первого запуска необходимо установить параметры системы, выбрав пункт меню “Login & configure”.

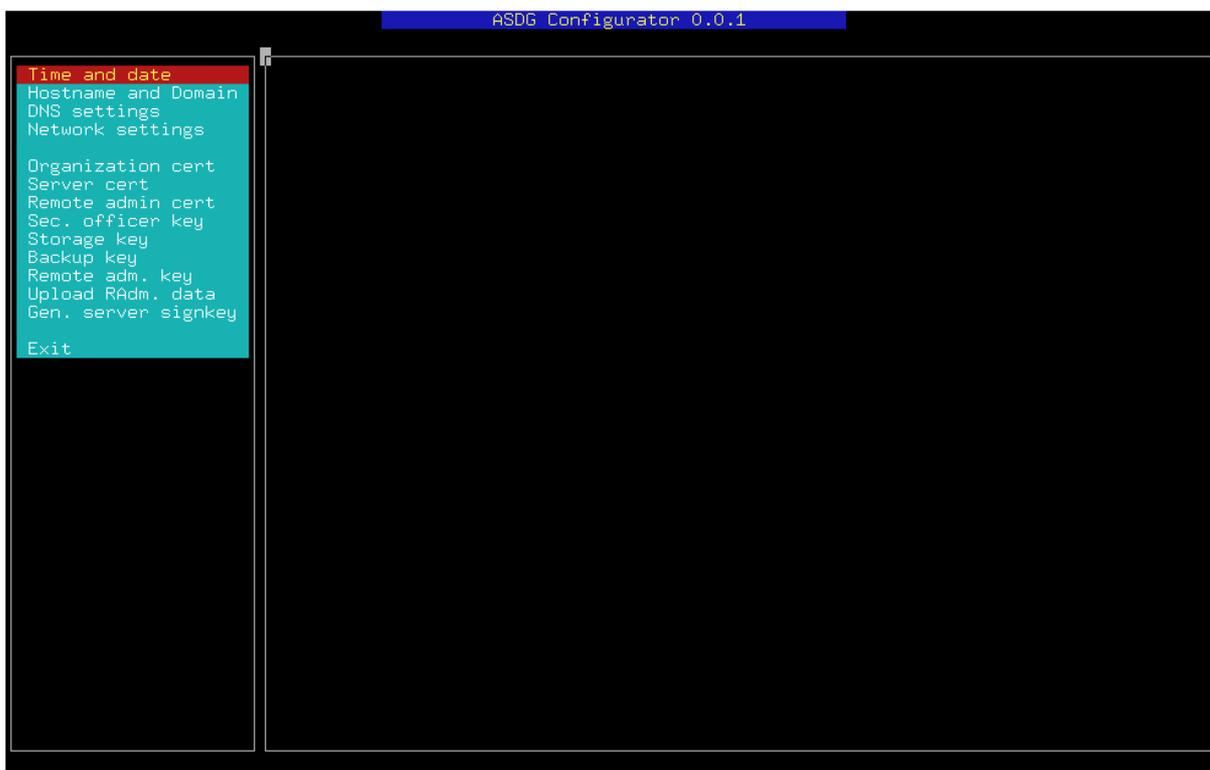


Рис. 4. Окно конфигуратора локальной консоли управления

В новом окне отображаются следующие пункты меню, которые при первом запуске системы необходимо выполнить в строгой последовательности, заполняя каждое поле в отображаемых диалоговых окнах:

- в.1) установка текущего времени и даты
- в.2) установка сетевого имени и домена
- в.3) установка адресов сервера DNS
- в.4) настройка параметров сетевых интерфейсов для подключения к глобальной и локальной сетям
- в.5) создание сертификата организации
- в.6) создание сертификата сервера
- в.7) создание сертификатов удаленных администраторов
- в.8) создание ключа офицера безопасности
- в.9) создание ключа хранения
- в.10) создание ключа резервного копирования
- в.11) создание ключей удаленных администраторов
- в.12) снятие ключевых данных удаленных администраторов на USB-совместимый носитель
- в.13) создание секретного ключа подписи сервера

По завершении ввода параметров системы необходимо выбрать соответствующий пункт меню “Exit” для возврата к основному интерфейсному окну.

При помощи ключевых данных удаленных администраторов становится возможным взаимодействие с веб-интерфейсом конфигурирования системы с удаленного рабочего места для управления задачами (см. 3.4.) .

2.7.6.2. Последующие запуски системы

а) параметры системы были определены ранее. В ответ на приглашение необходимо приложить к считывателю ТМ-носитель с ключом офицера безопасности

б) 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.

3.3. 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),

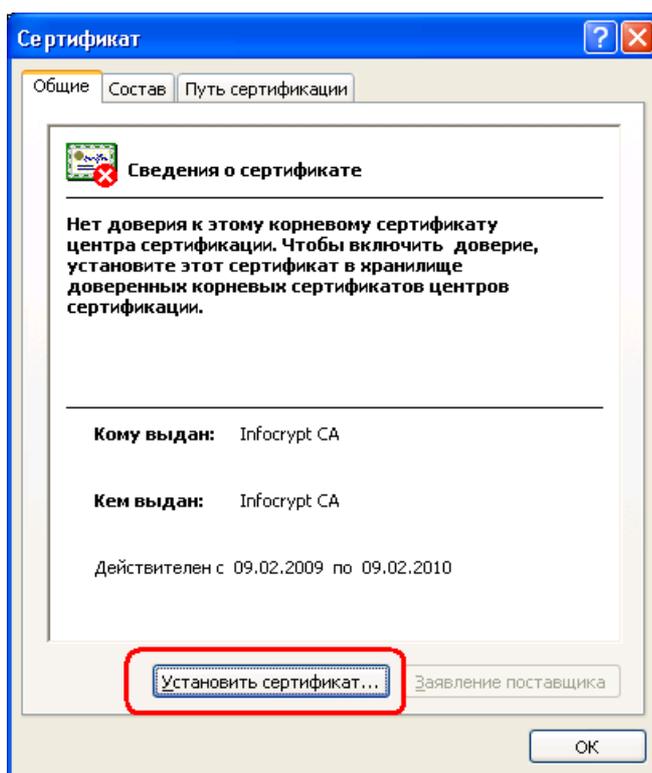
- отображением пунктов меню веб-интерфейса удаленного администрирования.

3.4. Настройка удаленного доступа

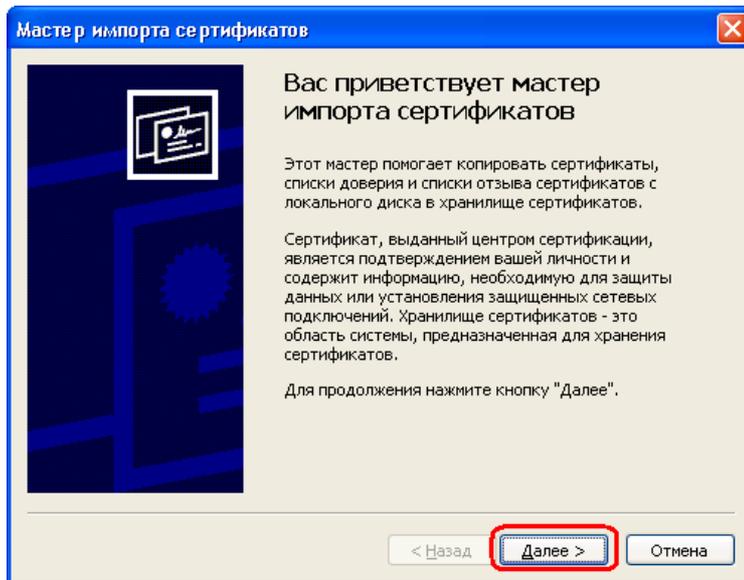
Для осуществления удаленного доступа к ПФО администратор должен иметь сертификат организации, а также заверенный им собственный сертификат. Оба сертификата администратор формирует на сервере с помощью меню конфигуратора. Затем, посредством того же меню, администратор забирает их на USB-совместимом носителе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

3.4.1. Установка сертификата организации.

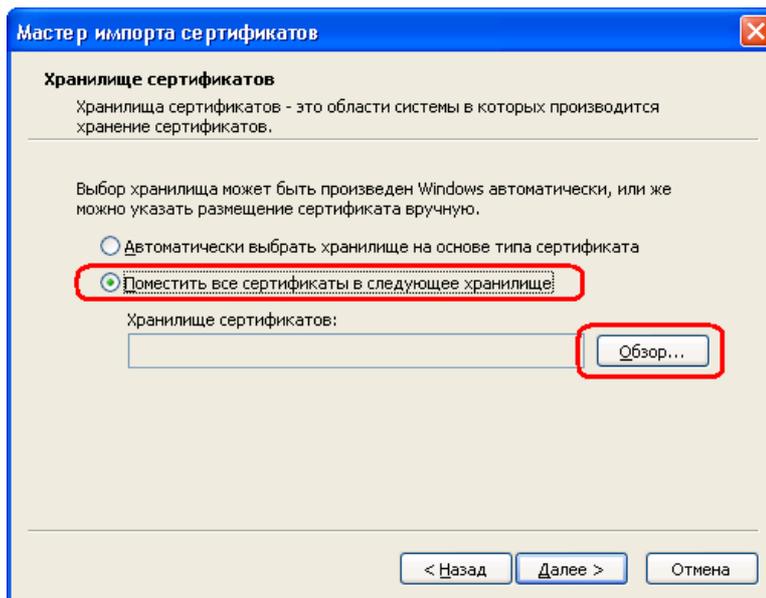
1. При помощи любого файлового менеджера администратор находит на носителе, содержащем сертификаты, файл с сертификатом организации **org.crt** и активирует процесс установки, открывая этот файл (двойным кликом по нему или нажатием клавиши «Ввод»). Появляется следующее окно-предложение:



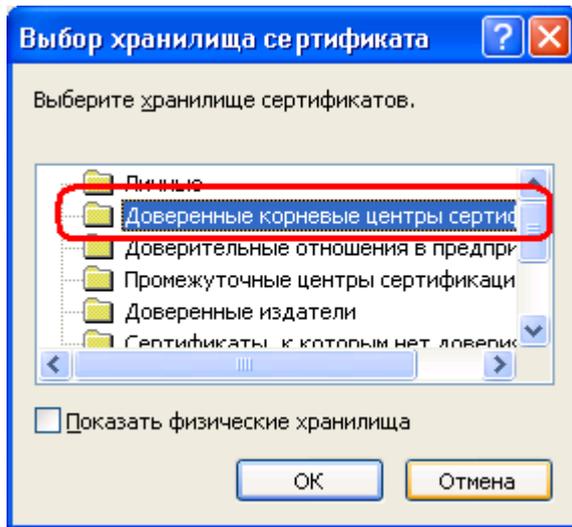
2. Выбираем пункт «Установить сертификат». Запускается мастер импорта сертификатов. Нажимаем на кнопку «Далее».



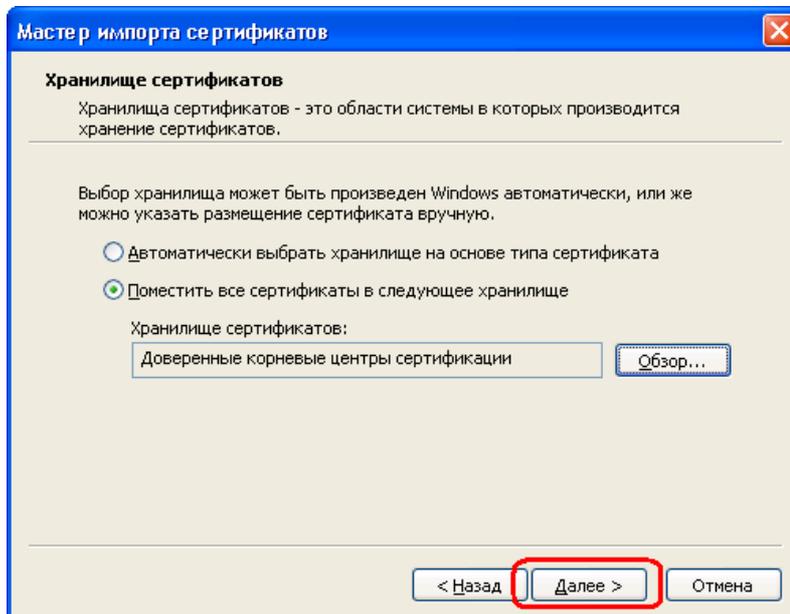
3. Появляется предложение о выборе хранилища для сертификата. Выбираем пункт «Поместить все сертификаты в следующее хранилище». Нажимаем на кнопку «Обзор».



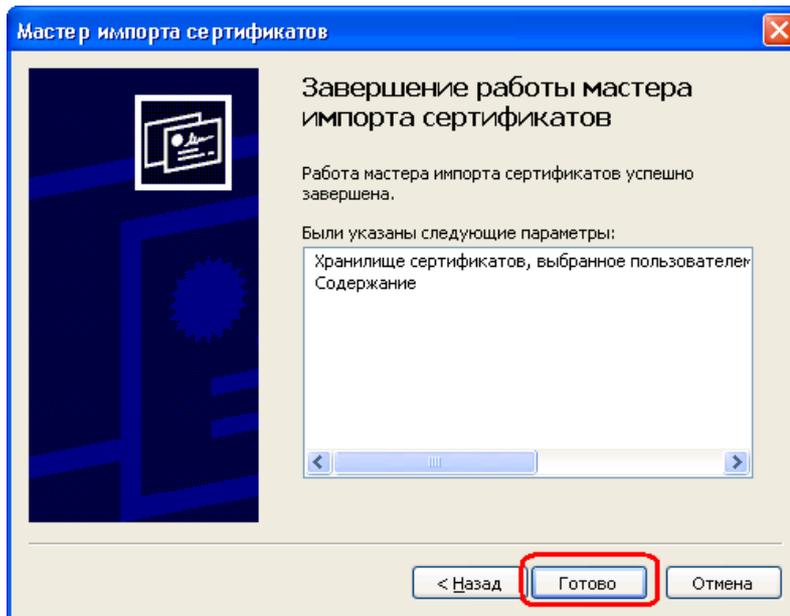
4. Появляется окно выбора хранилища. Выбираем пункт «Доверенные корневые центры сертификации».



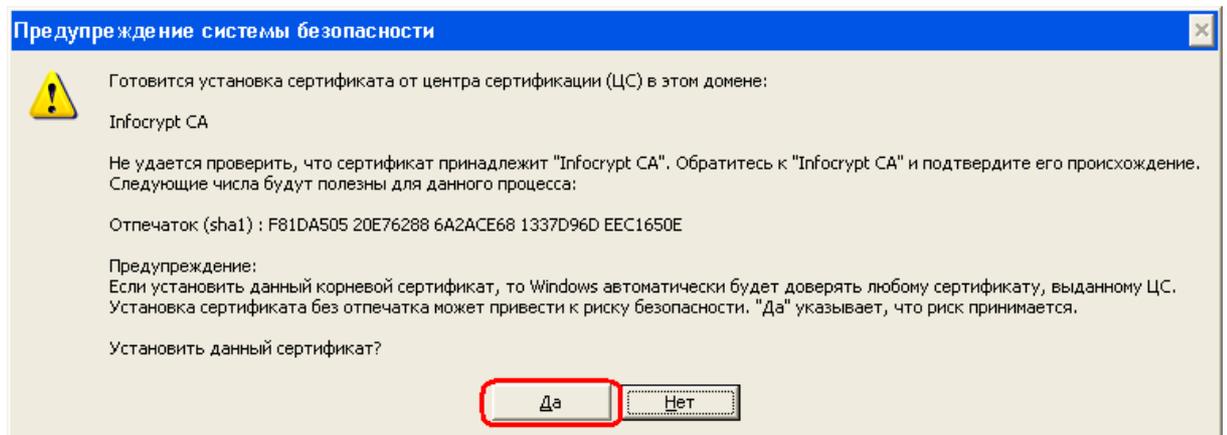
5. Нажимаем на кнопку «Далее».



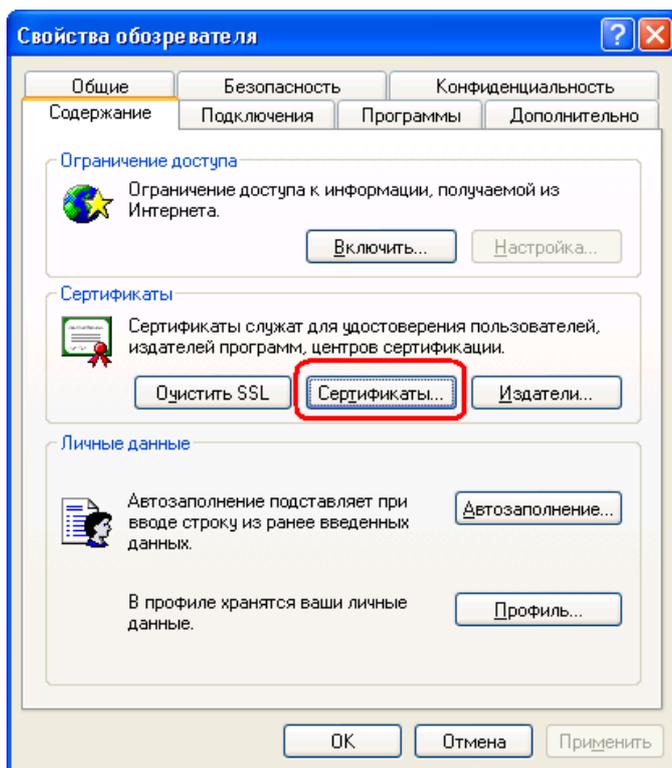
6. Мастер импорта сертификатов завершает свою работу. Нажимаем на кнопку «Готово».



7. Появляется предупреждение системы безопасности. Нажимаем на кнопку «Да».

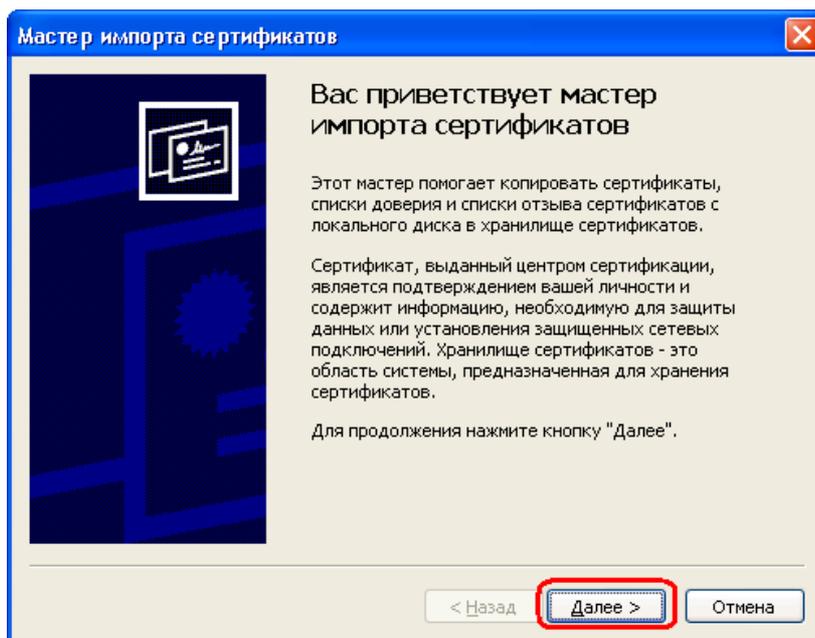


Теперь импорт сертификата организации успешно завершён, о чём система выдает соответствующее сообщение. Посмотреть установленный сертификат организации можно, например, с помощью браузера Internet Explorer, выбрав в свойствах обозревателя закладку «Содержание», и на ней нажав кнопку «Сертификаты».

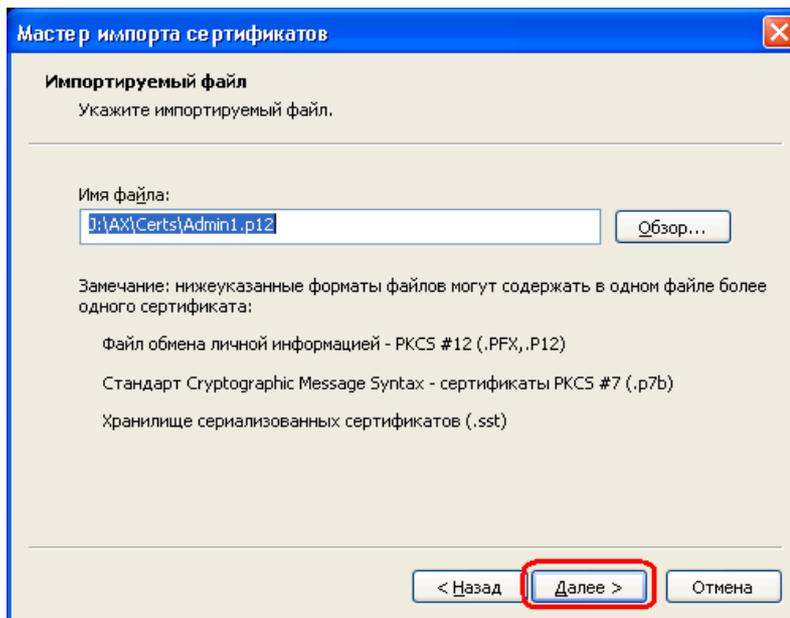


3.4.2. Установка сертификата администратора.

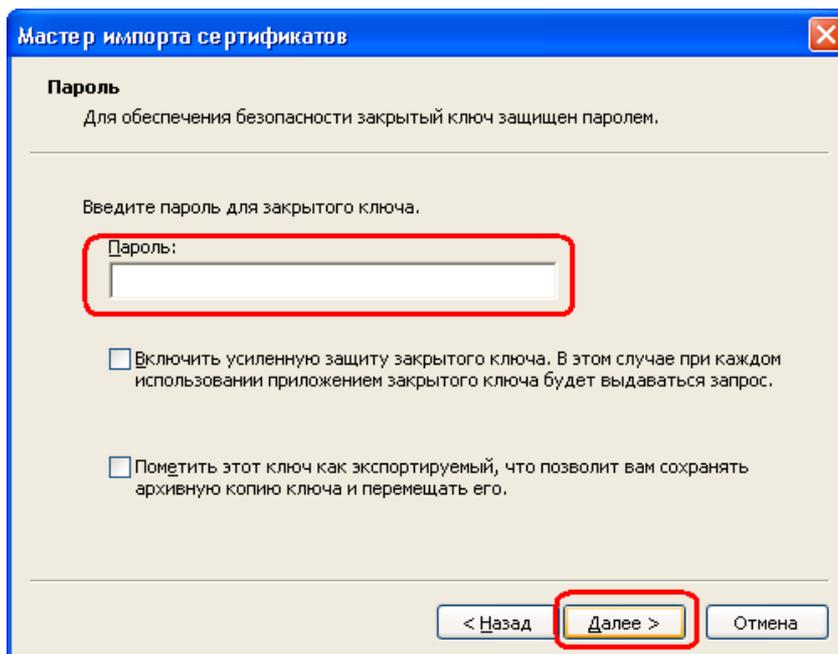
1. При помощи любого файлового менеджера администратор находит на носителе, содержащем сертификаты, файл со своим сертификатом **AdminN.p12** (N – порядковый номер администратора) и активирует процесс установки, открывая этот файл (двойным кликом по нему или нажатием клавиши «Ввод»). Запускается мастер импорта сертификатов:



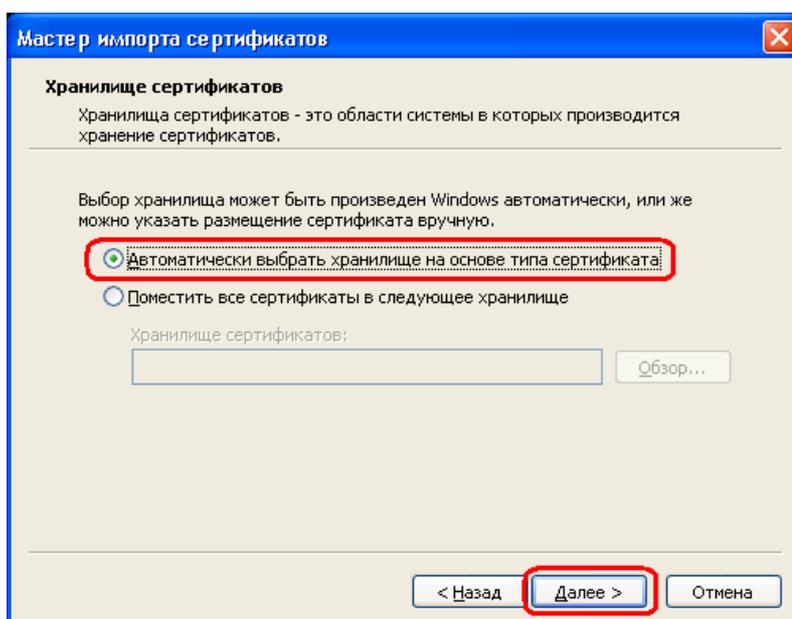
2. Нажимаем на кнопку «Далее». В открывшемся окне подтверждаем выбранный файл с сертификатом нажатием на кнопку «Далее».



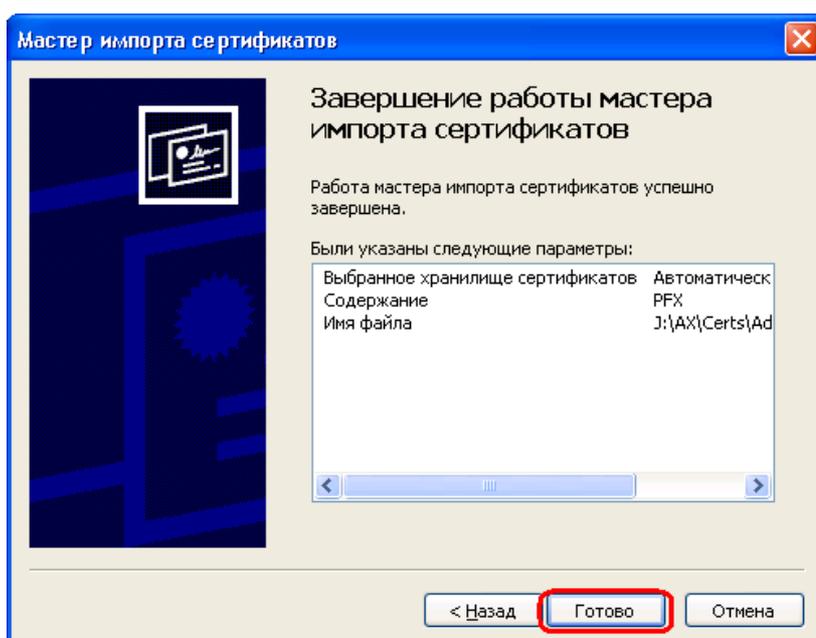
3. Следующее окно предлагает ввести пароль секретного ключа. После ввода нажимаем на кнопку «Далее».



4. Выбираем хранилище сертификатов. Необходимо отметить пункт «Автоматически выбрать хранилище на основе типа сертификата». Нажимаем на кнопку «Далее».



5. Мастер импорта сертификатов завершает свою работу. Нажимаем на кнопку «Готово».



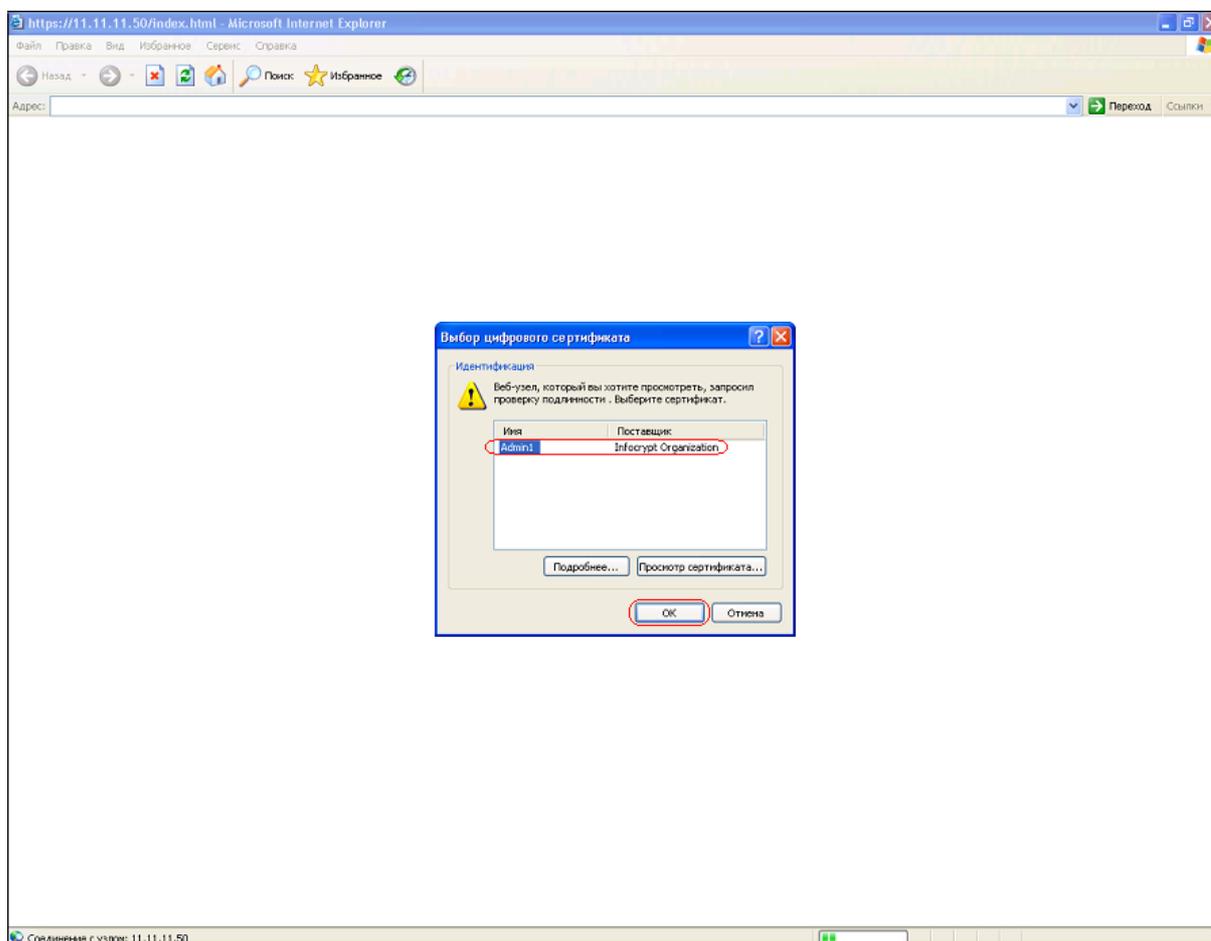
Импорт сертификата администратора успешно завершается, о чем система выдаст соответствующее сообщение. Посмотреть установленный сертификат администратора можно так же, как и сертификат организации, с помощью браузера Internet Explorer.

3.4.3. Запуск системы удаленного администрирования.

Удаленный доступ к интерфейсу конфигурирования ПФО 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.

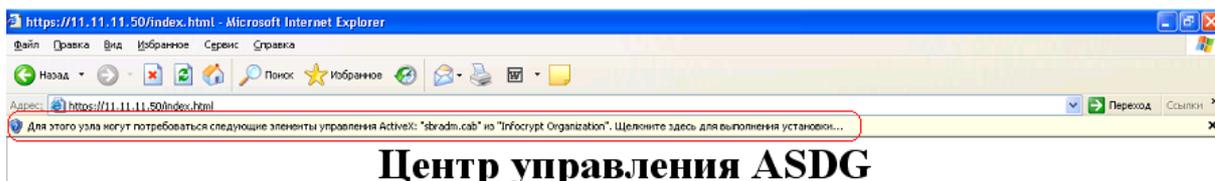
При попытке соединения с ПФО веб-браузер (по умолчанию Internet Explorer) предложит выбрать сертификат, который будет предъявлен серверу для аутентификации. Из списка необходимо выбрать сертификат, установленный в пункте 3.4.2. данной инструкции, т.е. сертификат администратора, и нажать на кнопку «ОК».



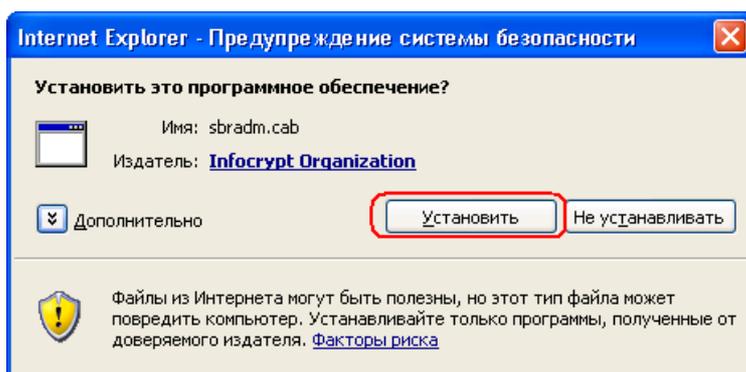
После успешного соединения с ПФО администратор обязан проверить отпечаток предъявленного ему сертификата сервера, сравнив его с тем, который был ему предоставлен при создании его собственного сертификата (сертификата администратора). Можно это сделать, щелкнув по значку замка в правой части нижней строки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

3.4.4. 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:



После согласия на установку, система выведет окно предупреждения системы безопасности. Здесь можно получить информацию как о самой компоненте, щелкнув по ее наименованию, так и о сертификате, которым она подписана, щелкнув, соответственно, по ссылке на издателя. Затем нажимаем на кнопку «Установить».



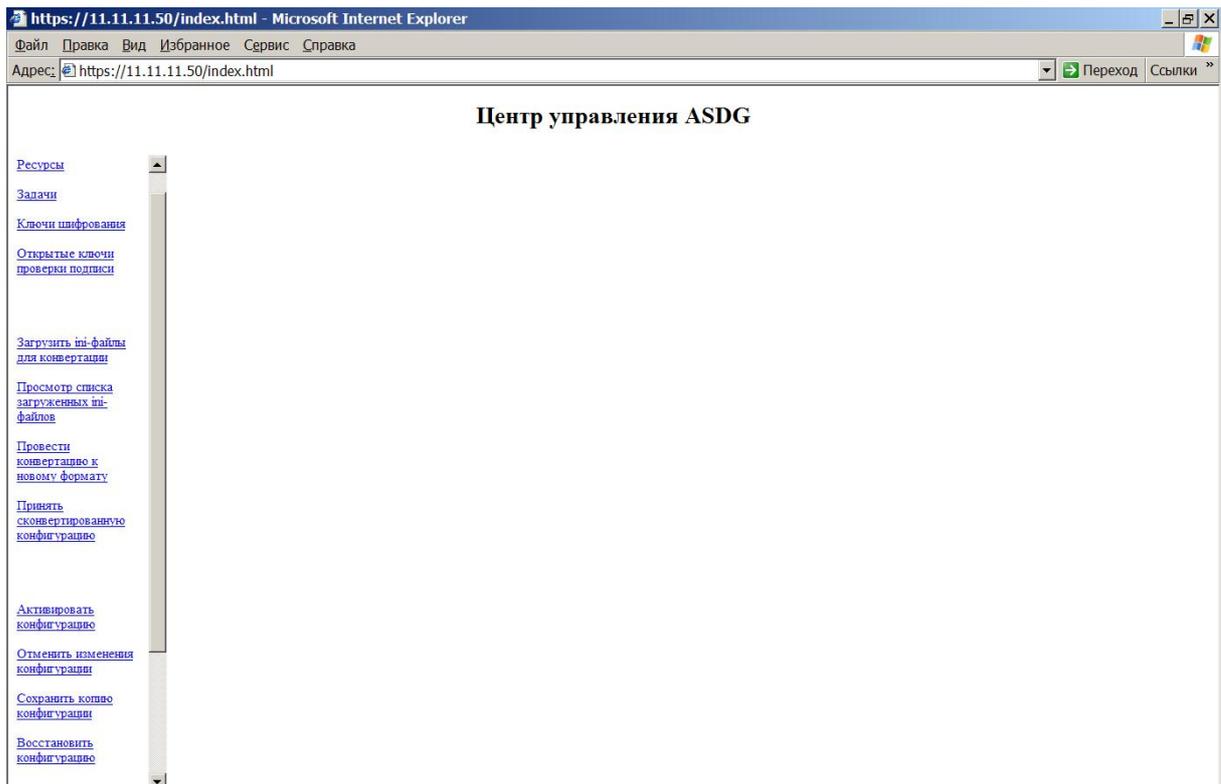
Для выполнения операции шифрования также необходим файл с открытым ключом сервера **Server.pkb**. Этот файл администратор должен был получить в процессе создания своего удаленного ключа. Файл **Server.pkb** нужно переместить в каталог установки ActiveX компоненты (по умолчанию «*%Системный диск %\Infocrypt\RemoteAdmin*»).

4 КОНФИГУРИРОВАНИЕ

Для выполнения действий по конфигурированию ПФО с удаленного рабочего места необходимо предварительно настроить систему безопасности удаленного ПК для корректной аутентификации при установлении соединения с ПФО (см. 3.4.).

Удаленный доступ к интерфейсу конфигурирования ПФО осуществляется средствами веб-браузера. Для этого браузеру необходимо дать команду на открытие URL вида

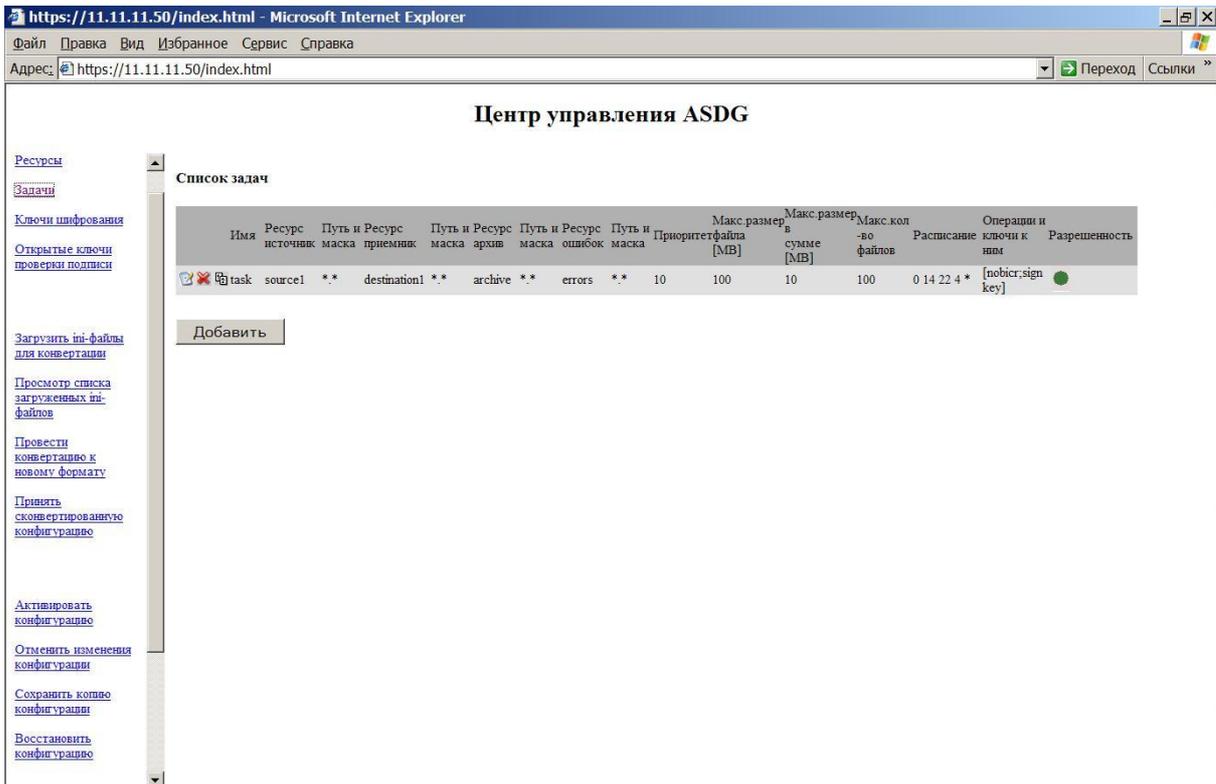
`https://<сетевое имя ПФО>/index.html`



Веб-интерфейс конфигурирования и управления предоставляет нижеперечисленные возможности по определению задач и графика обработки данных средствами ПФО.

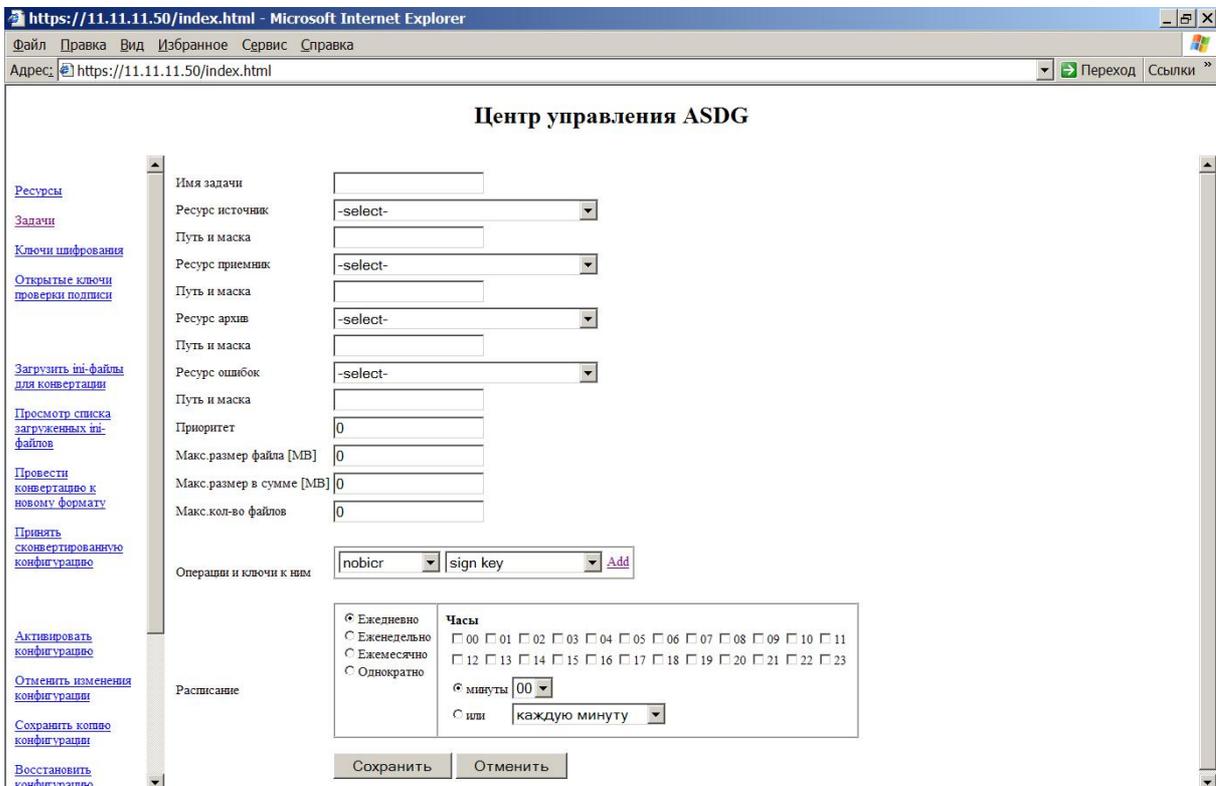
4.1. Управление задачами обработки

Для просмотра списка существующих задач обработки данных необходимо выбрать пункт меню (колонка слева) «Задачи». В поле по центру будет отображена таблица, строки которой описывают задачи, а столбцы – параметры данных задач.



4.1.1. Добавление новой задачи

Открытие новой страницы для добавления задачи происходит при нажатии на кнопку «Добавить», которая отображается под таблицей с параметрами задач.



При добавлении необходимо определить параметры задачи и нажать на кнопку «Сохранить» для подтверждения или «Отменить» для отмены.

4.1.2. Удаление задачи

В таблице задач слева от каждой строки расположена кнопка с пиктограммой



, нажатие на которую повлечет удаление данной задачи.

4.1.3. Редактирование задачи

В таблице задач слева от каждой строки расположена кнопка с пиктограммой



, нажатие на которую позволит выполнить редактирование параметров данной задачи. При этом на экране отображается страница с параметрами задачи, которые можно изменять.

При завершении редактирования необходимо нажать на кнопку «Сохранить» для подтверждения изменений или на кнопку «Отменить» для отмены.

4.1.4. Создание копии задачи

В таблице задач слева от каждой строки расположена кнопка с пиктограммой



, предназначенная для дублирования соответствующей задачи. Если нажать на нее, на экране появится страница с параметрами новой задачи, которые можно изменять. Изначально параметры задачи-копии совпадают с параметрами исходной задачи.

По завершении определения параметров задачи-копии необходимо нажать на кнопку «Сохранить» для их сохранения и добавления задачи к списку задач, или на кнопку «Отменить» для отмены создания копии.

4.2. Управление сетевыми ресурсами

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

The screenshot shows the 'Центр управления ASDG' interface in Microsoft Internet Explorer. The browser address bar shows 'https://11.11.11.50/index.html'. The page title is 'Центр управления ASDG'. On the left, there is a navigation menu with links: 'Ресурсы', 'Задачи', 'Ключи шифрования', 'Открытые ключи проверки подписи', 'Загрузить ini-файлы для конвертации', 'Просмотр списка загруженных ini-файлов', 'Провести конвертацию к новому формату', 'Принять сконвертированное конфигурацию', 'Активировать конфигурацию', 'Отменить изменения конфигурации', 'Сохранить копию конфигурации', and 'Восстановить конфигурацию'. The main content area is titled 'Список ресурсов' and contains a table with the following data:

Имя	URL	Транспорт	Таймаут	Учетная запись	Пароль	Рекурсивно	Доступность	Разрешенность
source1	//11.11.11.18/src1/	cifs	5	aist	12345	None		
destination1	//11.11.11.18/dst1/	cifs	5	aist	12345	None		
errors	//11.11.11.18/err/	cifs	5	aist	12345	None		
archive	//11.11.11.18/arch/	cifs	5	aist	12345	None		

Below the table is a 'Добавить' button.

4.2.1. Добавление нового ресурса

Открытие новой страницы для добавления ресурса происходит при нажатии на кнопку «Добавить», которая отображается под таблицей с параметрами ресурсов.

The screenshot shows the 'Центр управления ASDG' interface in Microsoft Internet Explorer. The browser address bar shows 'https://11.11.11.50/index.html'. The page title is 'Центр управления ASDG'. On the left, there is a navigation menu with links: 'Ресурсы', 'Задачи', 'Ключи шифрования', 'Открытые ключи проверки подписи', 'Загрузить ini-файлы для конвертации', 'Просмотр списка загруженных ini-файлов', 'Провести конвертацию к новому формату', 'Принять сконвертированное конфигурацию', 'Активировать конфигурацию', 'Отменить изменения конфигурации', 'Сохранить копию конфигурации', and 'Восстановить конфигурацию'. The main content area is titled 'Центр управления ASDG' and contains a form for adding a new resource with the following fields:

- Имя ресурса:
- URL:
- Транспорт:
- Учетная запись:
- Пароль:
- Таймаут:
- Рекурсивно:

Below the form are two buttons: 'Сохранить' and 'Отменить'.

При добавлении необходимо определить параметры ресурса и нажать на кнопку «Сохранить» для подтверждения или «Отменить» для отмены.

4.2.2. Удаление ресурса

В таблице ресурсов слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую повлечет удаление данного ресурса из списка ресурсов. Если ресурс используется какой-либо задачей, его удаление невозможно; конфигуратор выдаст сообщение об ошибке.

4.2.3. Редактирование ресурса

В таблице ресурсов слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую позволит выполнить редактирование данного ресурса. При этом на экране отображается страница с параметрами ресурса, которые можно изменять.

При завершении редактирования необходимо нажать на кнопку «Сохранить» для подтверждения изменений или на кнопку «Отменить» для отмены.

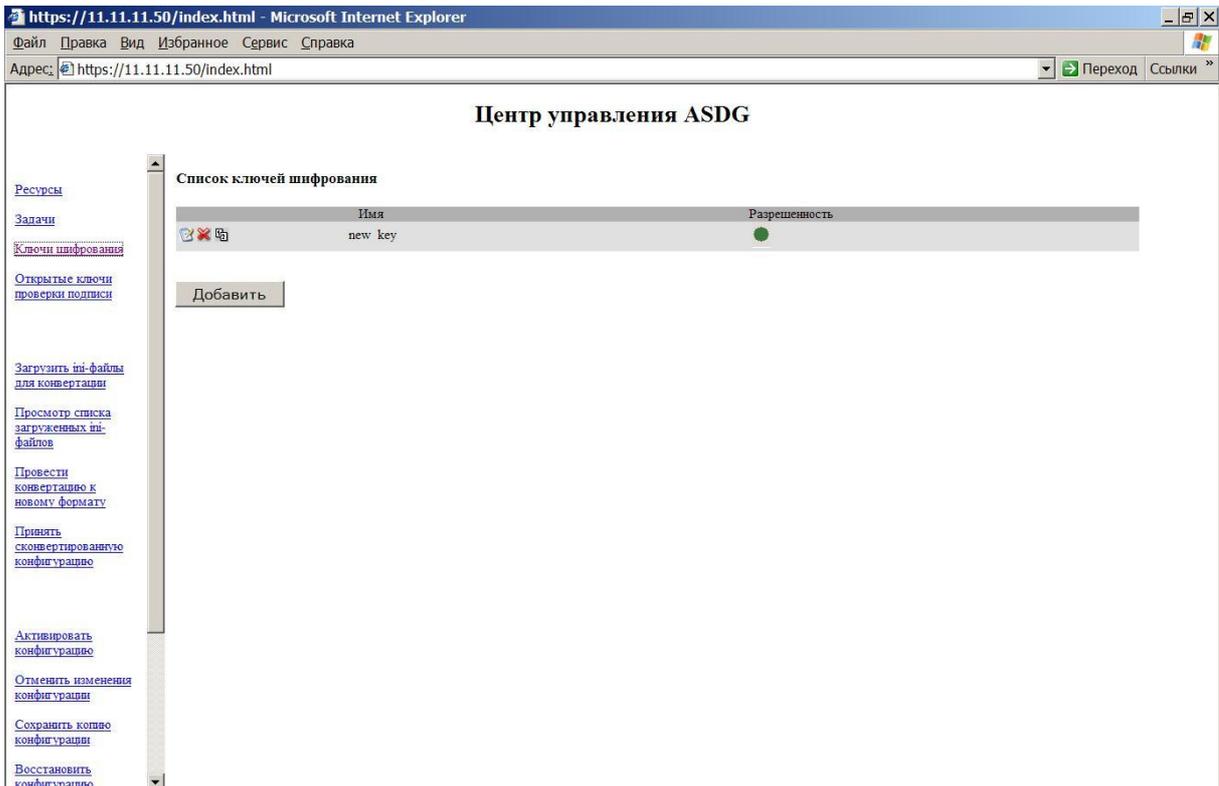
4.2.4. Создание копии ресурса

В таблице ресурсов слева от каждой строки расположена кнопка с пиктограммой , предназначенная для дублирования соответствующего ресурса. Если нажать на нее, 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 необходимо нажать на кнопку «Сохранить» для их сохранения и добавления ресурса к списку ресурсов, или на кнопку «Отменить» для отмены создания копии.

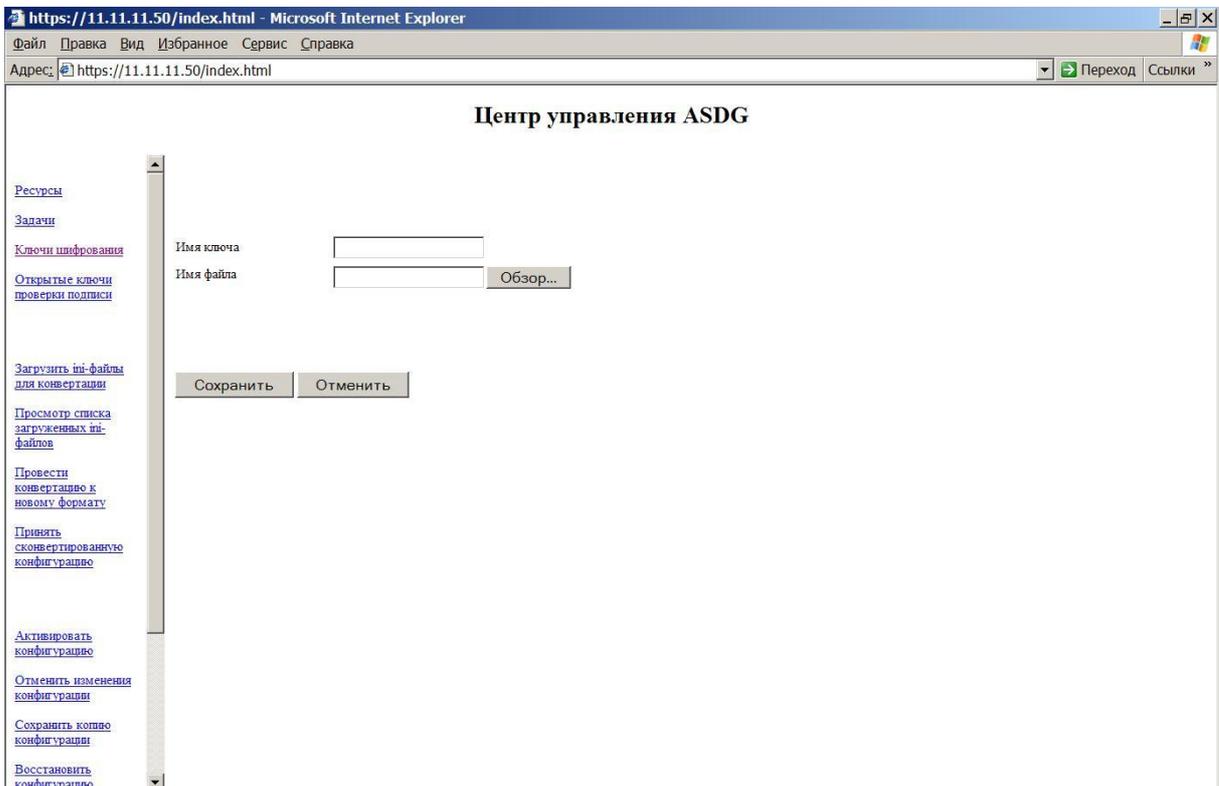
4.3. Управление ключами шифрования

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.



4.3.1. Добавление нового ключа шифрования

Открытие новой страницы для установки ключа шифрования происходит при нажатии на кнопку «Добавить», которая отображается под таблицей с параметрами ключей.



При добавлении необходимо определить имя ключа, указать файл и нажать на кнопку «Сохранить» для подтверждения или на кнопку «Отменить» для отмены.

4.3.2. Удаление ключа шифрования

В таблице ключей шифрования слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую повлечет удаление данного ключа.

Если ключ используется какой-либо задачей, его удаление невозможно; конфигуратор выдаст сообщение об ошибке.

4.3.3. Редактирование ключа шифрования

В таблице ключей шифрования слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую позволит выполнить редактирование данного ключа. При этом на экране отображается страница, предоставляющая возможность изменить имя ключа, а также указать новый файл ключа шифрования.

При завершении редактирования необходимо нажать на кнопку «Сохранить» для подтверждения или на кнопку «Отменить» для отмены.

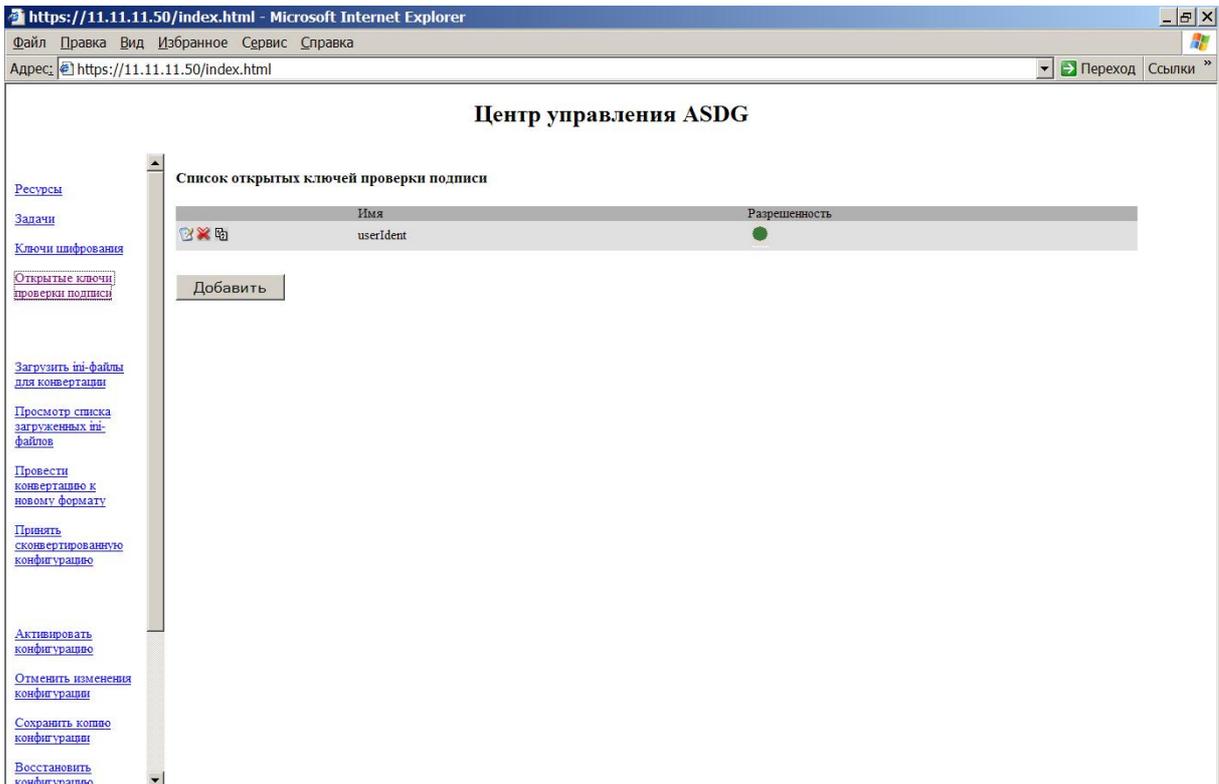
4.3.4. Создание копии ключа шифрования

В таблице ключей шифрования слева от каждой строки расположена кнопка с пиктограммой , предназначенная для дублирования соответствующего ключа. Если нажать на нее, 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 необходимо нажать на кнопку «Сохранить» для их сохранения и добавления ключа к списку ключей шифрования, или на кнопку «Отменить» для отмены создания копии.

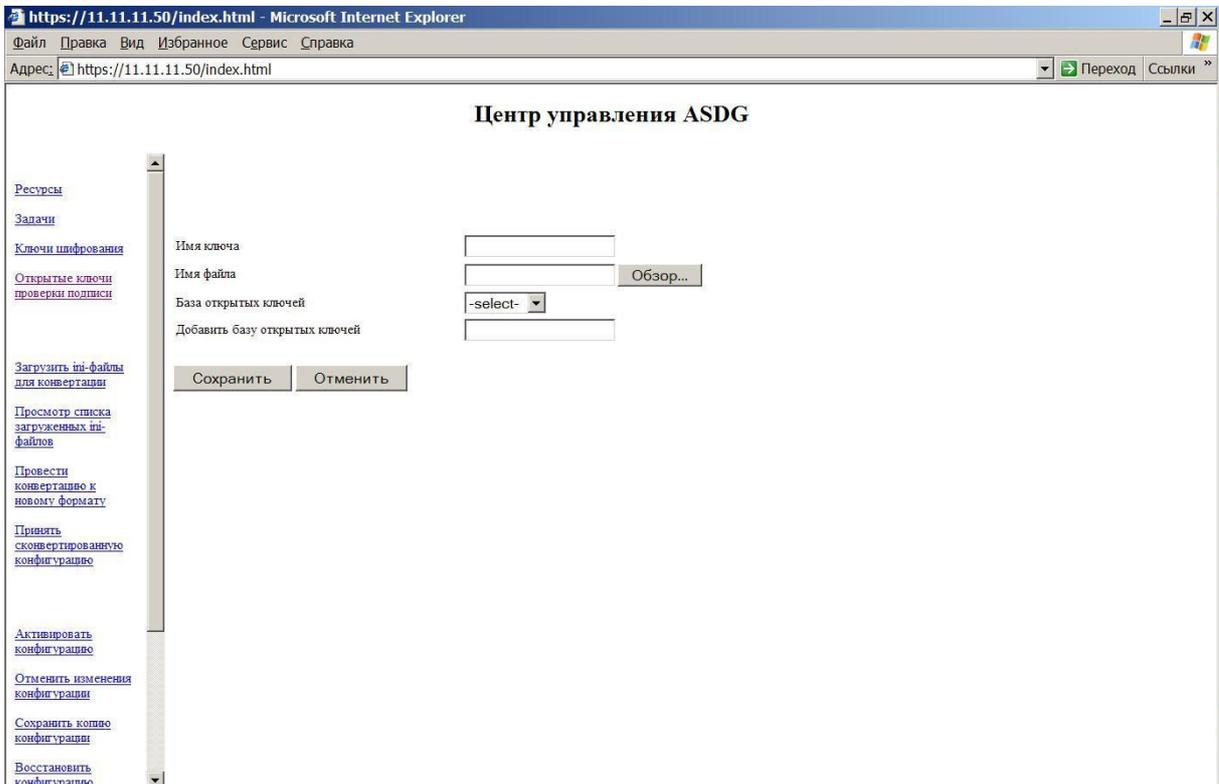
4.4. Управление ключами проверки подписи

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.



4.4.1. Добавление нового ключа проверки подписи

Открытие новой страницы для установки ключа проверки подписи происходит при нажатии на кнопку «Добавить», которая отображается под таблицей с параметрами ключей.



При добавлении необходимо определить имя ключа, указать файл ключа, выбрать базу открытых ключей, куда следует добавить ключ, и нажать на кнопку «Сохранить» для подтверждения или на кнопку «Отменить» для отмены.

4.4.2. Удаление ключа проверки подписи

В таблице ключей проверки подписи слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую повлечет удаление данного ключа.

Если ключ используется какой-либо задачей, его удаление невозможно; конфигуратор выдаст сообщение об ошибке.

4.4.3. Редактирование ключа проверки подписи

В таблице ключей шифрования слева от каждой строки расположена кнопка с пиктограммой , нажатие на которую позволит выполнить редактирование данного ключа. При этом на экране отображается страница, предоставляющая возможность изменить имя ключа, указать новый файл ключа шифрования и выбрать базу открытых ключей для сохранения ключа в данную базу.

При завершении редактирования необходимо нажать на кнопку «Сохранить» для подтверждения или на кнопку «Отменить» для отмены.

4.4.4. Создание копии ключа проверки подписи

В таблице ключей проверки подписи слева от каждой строки расположена кнопка с пиктограммой , предназначенная для дублирования соответствующего ключа. Если нажать на нее, на экране появится страница с параметрами ключа-копии, которые можно изменять. Изначально параметры ключа-копии совпадают с параметрами исходного ключа.

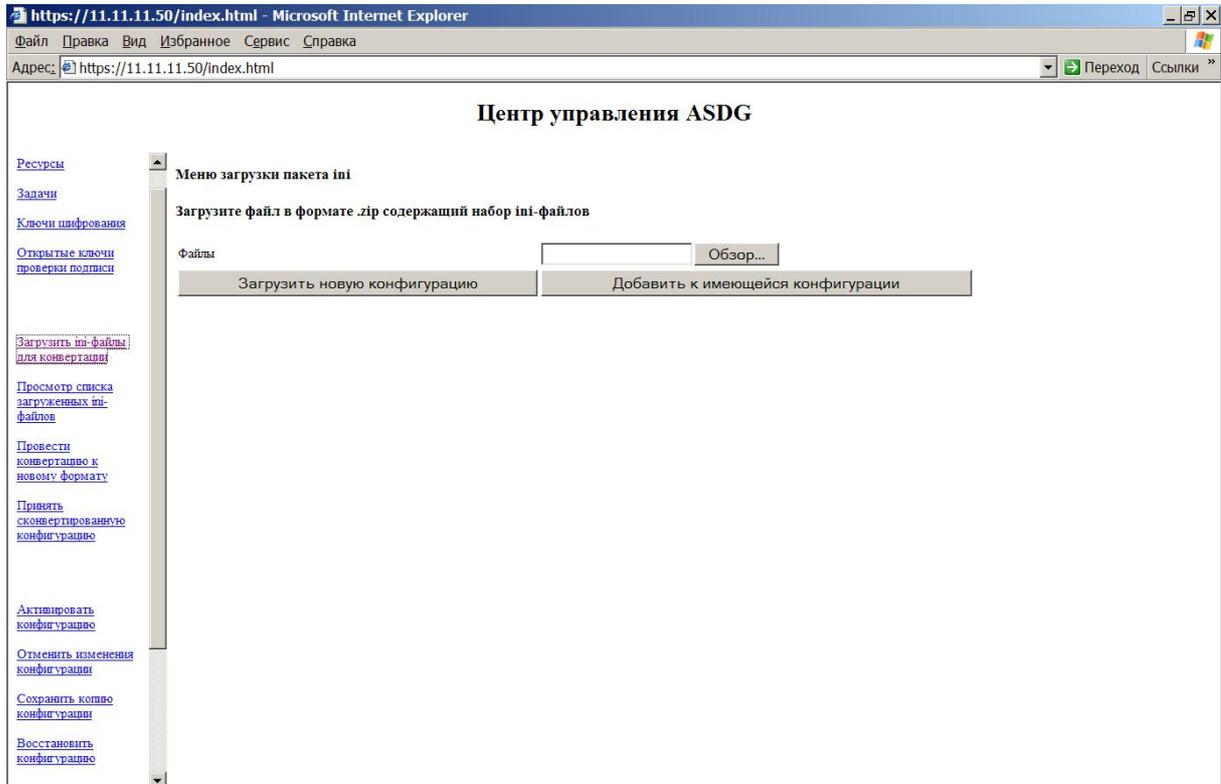
По завершении определения параметров ключа-копии необходимо нажать на кнопку «Сохранить» для их сохранения и добавления ключа к списку ключей проверки подписи, или на кнопку «Отменить» для отмены создания копии.

4.5. Конвертация конфигурационных файлов к новому формату

Предусмотрена возможность конвертации ini-файлов, содержащих параметры конфигурации, к новому формату. Для этого необходимо загрузить соответствующие файлы, провести конвертацию и средствами web-интерфейса доработать результат конвертации.

4.5.1. Загрузка ini-файлов для конвертации.

Чтобы загрузить ini-файлы для конвертации, нужно в меню слева выбрать пункт «Загрузить ini-файлы для конвертации». В центральной части экрана появится меню загрузки пакета ini.



Нужно указать zip-архив, содержащий необходимые ini-файлы, а так же один из двух способов загрузки.

Если нажать на кнопку «Загрузить новую конфигурацию», то прежде загруженные ini-файлы будут удалены, новые ini-файлы будут распакованы из выбранного архива.

Если нажать на кнопку «Добавить к имеющейся конфигурации», то новые ini-файлы будут распакованы из выбранного архива и добавлены к загруженным ранее ini-файлам.

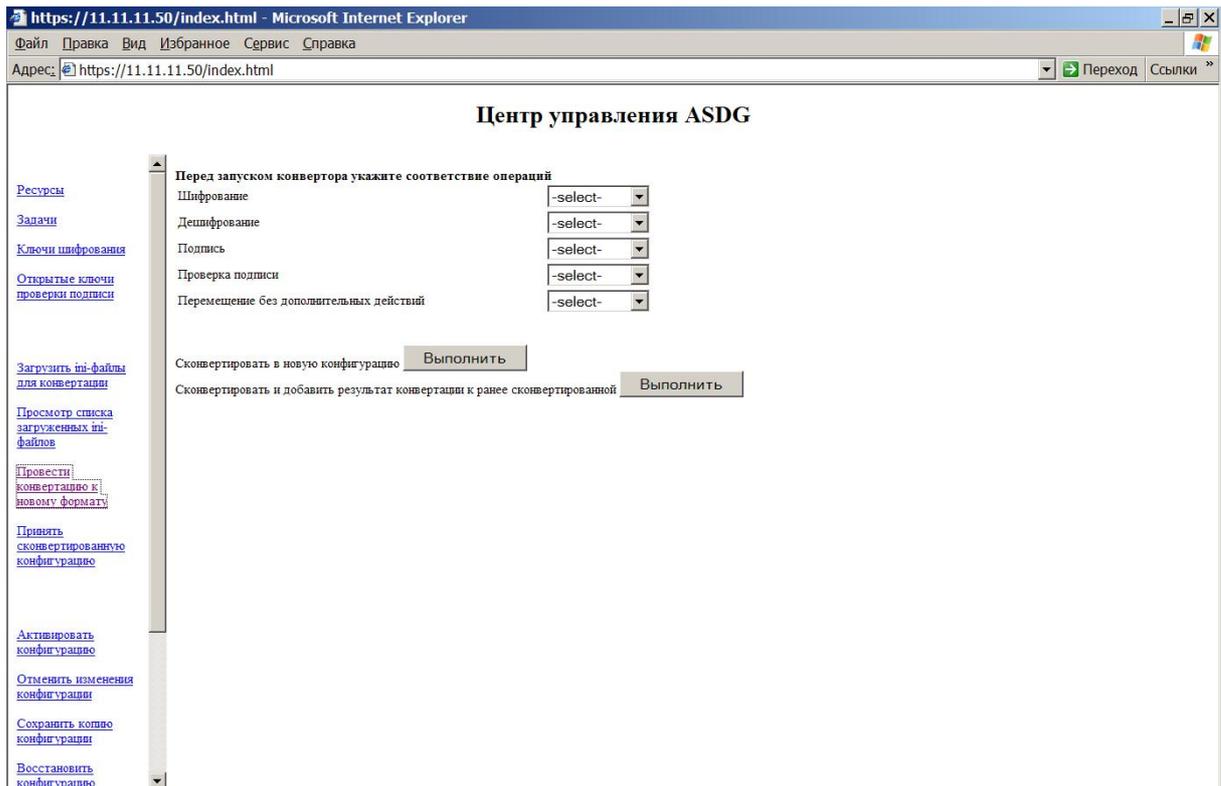
Если загрузка прошла успешно, то на экране появляется сообщение «Загрузка завершена», список всех загруженных ini-файлов и кнопка «Назад», позволяющая вернуться в меню загрузки.

4.5.2. Просмотр списка загруженных ini-файлов

Если выбрать пункт меню «Просмотр списка загруженных ini-файлов», то в центральной части страницы будет отображен список загруженных ранее файлов.

4.5.3. Конвертация к новому формату

Чтобы провести конвертацию загруженных ini-файлов к новому формату, нужно выбрать соответствующий пункт в меню слева.



Перед запуском конвертора необходимо установить смысловое соответствие операций, выбрав для каждой из них операцию из выпадающего списка.

Далее нужно выбрать способ конвертации и запустить конвертор, нажав на кнопку «Выполнить».

Если выбрать первый способ («Сконвертировать в новую конфигурацию»), то произойдет конвертация загруженных ini-файлов к новому формату. Результатом этой операции будет новая конфигурация, параметры которой будут получены из загруженных ini-файлов.

Если выбрать второй способ («Сконвертировать и добавить результат конвертации к ранее сконвертированной»), то конфигурация, являющаяся результатом предыдущей конвертации, будет дополнена параметрами, полученными из загруженных ini-файлов.

Чтобы просматривать и править конфигурацию, полученную конвертацией ini-файлов, нужно ее принять.

4.5.4. Сохранение результата конвертации для дальнейшей доработки.

Если выбрать пункт меню слева «Принять сконвертированную конфигурацию» и нажать на появившуюся кнопку «Сохранить», текущая конфигурация будет замещена результатом конвертации загруженных ini-файлов. После этого сконвертированная конфигурация становится доступной для просмотра и необходимых правок.

В редактировании будут нуждаться параметры тех ресурсов (ключей, задач), у которых в таблице ресурсов (ключей или задач, соответственно) в графе «Разрешенность» будет выставлено значение . Если нажать на кнопку с пиктограммой , то на экране появится сообщение, содержащее список нуждающихся в изменении параметров соответствующего ресурса (ключа, задачи).

4.6. Активация конфигурации

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

4.6.1. Отмена изменений

Возврат к последней активированной версии конфигурации после внесения правок в текущую осуществляется путем выбора пункта меню «Отменить изменения конфигурации». При этом необходимо подтвердить намерения нажатием на появившуюся в центральной части экрана кнопку «Отменить».

4.7. Создание резервной копии конфигурации

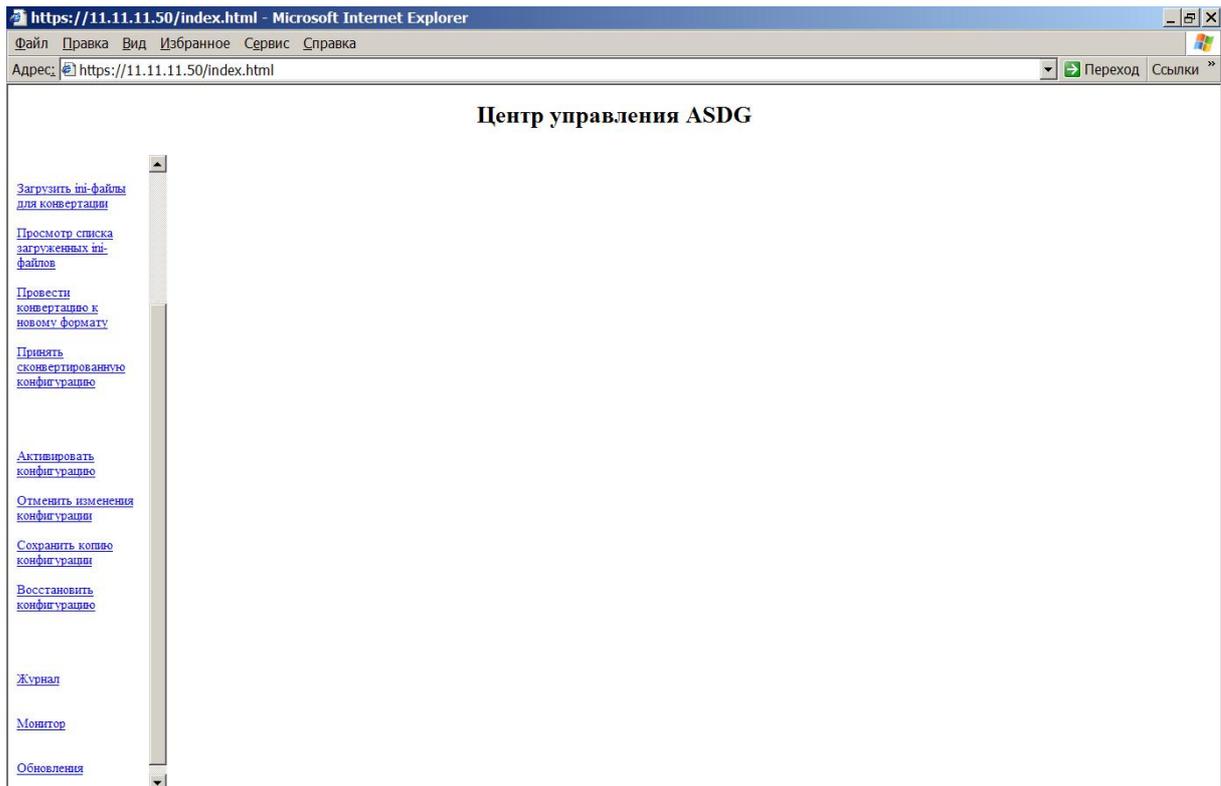
Предусмотрена возможность сохранения конфигурации ПАК ПФО для ее последующего восстановления по необходимости. Для этого нужно выбрать пункт меню веб-интерфейса удаленного администрирования «Сохранить копию конфигурации».

4.8. Восстановление конфигурации

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

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

5 МОНИТОРИНГ



5.1. Просмотр системного журнала

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

5.2. Просмотр текущего состояния системы

Перечень задач, которые обрабатываются ПФО в некоторый 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 ПФО возможно при помощи локальной консоли управления. Для этого нужно выбрать пункт меню «Turn off».

5.4. Перезагрузка системы

Перезагрузить ПАК ПФО возможно при помощи локальной консоли управления. Для этого нужно выбрать пункт меню «Reboot».

6 ОБНОВЛЕНИЕ

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 (мониторинг), о событиях, предшествовавших моменту возникновения проблем (журнал). Эти данные необходимо предоставить в службу технической поддержки.