Код безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

"Jinn-Server" версии 1.0

Руководство пользователя

RU.88338853.501430.009 01 92

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для пользователей изделия "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0" (далее – ПАК "Jinn-Server", комплекс, ПАК). В нем содержатся сведения, необходимые для эксплуатации ПАК "Jinn-Server".

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень курсов и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Основные понятия, термины и определения

Термин	Определение
ИОК/PKI	Инфраструктура открытых ключей – комплекс программных и/или программно-аппаратных средств и организационно-технических мероприятий по обеспечению использования криптографии с открытым ключом, управления этими ключами и сертификатами, в частности, для решения задач защищенного электронного документооборота
CAS	CRL Archiving Service – сервис, предназначенный для хранения и автоматического обновления списков отозванных сертификатов и обновлений к ним с целью последующего использования хранимых CRL другими компонентами ПАК
CFV	Cetificate Format Validation – составная часть сервиса SVS, предназначенная для проверки сертификатов открытых ключей на квалифицированность
CRL/COC	Список отозванных сертификатов (основной, регулярный)
deltaCRL	Обновление к COC, выпускаемое УЦ в интервале между выпусками COC
DMZ	Демилитаризованная зона, ДМЗ – технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана (файрвола) с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ
SS	SigningService – сервис, предназначенный для формирования ЭП под некоторыми данными
SVS	SignatureValidationService – сервис, предназначенный для проверки данных, подписанных ЭП
ГУЦ	Головной удостоверяющий центр
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭД	Электронный документ
ЭП	Электронная подпись

Глава 1
Назначение ПАК "Jinn-Server"

Функциональное и эксплуатационное назначение ПАК "Jinn-Server"

ПАК "Jinn-Server", а также набор дополнительных программных средств предназначены для выполнения функции автоматической проверки и формирования электронной подписи (ЭП) на электронных документах (ЭД) с сетевой выгрузкой результата во внешний сервис.

Функции ПАК "Jinn-Server" определяются задачами, решаемыми ПАК.

Общая схема развертывания компонентов ПАК и их взаимодействие с внешними информационными системами представлены на рисунке 1.

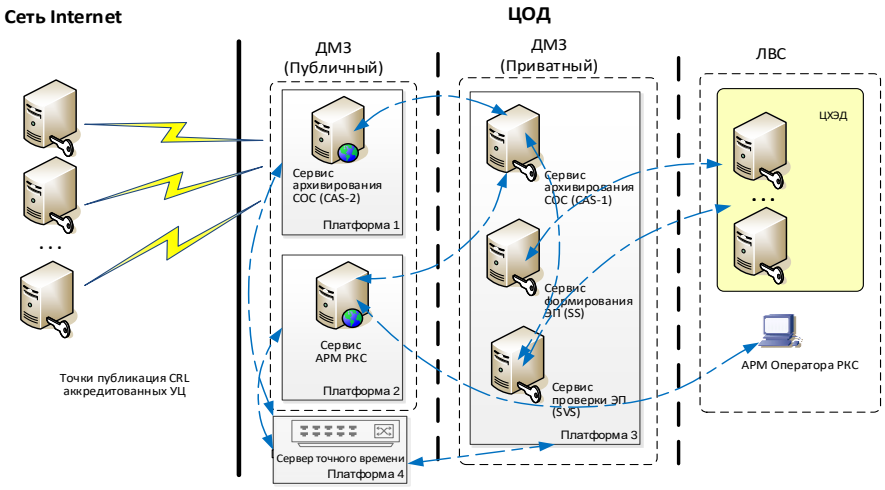

Рис. 1. Общая схема развертывания компонентов ПАК "Jinn-Server"

Примечание.

- При использовании кластеризации число необходимых узлов компонента CAS-2, размещаемого в DMZ, будет диктоваться в первую очередь соображениями обеспечения надежности ПАК и никак не связано с числом узлов ПАК, расположенных в защищенном сегменте сети.
- При использовании кластеризации возможно вынесение компонента CAS-1 на отдельный физический сервер. При этом доступ к функциям сервиса выполняется по протоколу TCP/IP.
- Настройки компонентов CAS-1 и CAS-2 позволяют дополнить существующий базовый транспорт в виде отчуждаемого носителя дополнительным онлайн-TCP-транспортом между компонентами.

ПАК "Jinn-Server" построен по модульному принципу и содержит в своем составе следующие компоненты (подсистемы):

- Сервис проверки ЭП (SVS – SignatureValidationService) – предназначен для проверки данных, подписанных ЭП, и проверки сертификатов ЭП на квалифицированность и действительность.
- Сервис формирования ЭП (SS – SigningService) – предназначен для формирования ЭП под некоторыми данными.
- Сервис архивирования CRL (CAS – CRLArchivingService) – предназначен для хранения и автоматического обновления списков отозванных сертификатов и обновлений к ним с целью последующего использования хранимых CRL другими компонентами ПАК. Этот сервис разделен на два модуля – внутренний сборщик CRL (CAS-1) и внешний (CAS-2).
- Подсистема администрирования – предназначена для мониторинга и управления компонентами ПАК.

Дополнительно:

1. Для сервисов подписи и проверки при работе с форматом WS-Security обеспечивается возможность работы с атрибутом "actor".
   - Для сервиса проверки: блок Signature подлежит проверке, если он сам или один из его родительских элементов (wsse:Security) содержит атрибут "actor", значение которого совпадает со значением аргумента "actor".
   - Для сервиса подписи: для сформированного блока ds:Security будет выбран в качестве родительского блока wsse:Security, имеющий атрибут "actor" со значением, равным значению аргумента "actor", передаваемого при вызове функции. Если такого блока нет, он должен быть создан. При создании блоку wsse:Security помимо атрибута "actor" со значением, равным значению аргумента "actor", будет присвоен атрибут wsu:Id со случайным, уникальным для данного XML-документа значением.
2. Для сервиса проверки в случае успешной обработки запроса на проверку xml-подписи в каждом элементе ответа SignatureInfo::SignatureRef всегда создается элемент xmlId со значением атрибута Id соответствующего проверенного элемента Signature.
3. При формировании списка доверенных издателей имеется возможность загрузки TSL-списка, формат которого должен соответствовать описанию, доступному по ссылке (http://e-trust.gosuslugi.ru/docs/TSLExt.1.0.xsd), которое основано на ETSI TS 102 231 V3.1.2 (2009-12) "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information". При этом обеспечивается:
   - автоматическое получение самого TLS-файла из места его публикации;
   - проверка авторства и целостности полученного TLS-файла (сертификат автора подписи должен доставляться доверенным образом и передаваться процедуре проверки TSL-файла через специальный интерфейс);
   - формирование на основе TSL-файла списка доверенных УЦ в хранилище ПАК "Jinn-Server".

   В административном интерфейсе ПАК "Jinn-Server" предусмотрены инструменты, позволяющие:
   - управлять адресом публикации TSL и режимом его скачивания;
   - осуществлять управляемую пообъектно загрузку данных из TSL.

   При этом возможности администратора при обработке издателей, представленных в TLS, обеспечиваются:
   - в процессе загрузки данных из TSL – возможностью отказаться от регистрации нового издателя (например, в случае ошибок в формате представления сертификата издателя);
   - в процессе управления зарегистрированными издателями – редактированием списка точек публикации COC и возможностью последующего импорта COC.
4. В рамках обеспечения поддержки TSL в ПАК "Jinn-Server" предусмотрена возможность установки и (в случае необходимости) замены самоподписанного сертификата головного УЦ (ГУЦ), а также сертификатов промежуточных издателей, которые должны использоваться в процессе проверки загружаемых TSL. Механизм управления указанными сертификатами отделен и независим от управления списком издателей сертификатов конечных пользователей.
5. Алгоритм построения и проверки цепочки сертификатов поддерживает цепочки сертификатов длиной более 1 с учетом следующих ограничений: по явному указанию обслуживающего персонала либо использовать, либо нет в процедуре построения цепочки атрибут authorityCertSerialNumber. Выбор режима построения цепочки сертификатов должен указываться в конфигурационном файле компонента SVS ПАК "Jinn-Server". Кроме того, данный алгоритм не предусматривает обработку полного списка расширений из RFC5280, влияющих на результат построения цепочки сертификатов, например, расширений CertificatePolicies, NameConstraints, PolicyConstraints, PolicyMappings, inhibitAnyPolicy и других.

6. Для обеспечения должной производительности, а также для снижения нагрузки на смежные системы штатная поддержка указания XSLT-преобразований в элементе ds:Transform в виде HTTP-адреса имеет механизм кеширования со средствами управления сроком хранения записей в xslt-кеше. Поддержка авторизации и защищенных соединений (https) не требуется.

Доступ к криптографическим функциям производится с использованием MicrosoftCryptoAPI для СКЗИ "КриптоПро CSP" для платформы Linux.

Сервис проверки ЭП (SVS)

SVS оформлен как веб-сервис для доступа по протоколу HTTP [2] через OSB (OracleServiceBus). SVS поддерживает:

- форматы подписи – CMS SignedData [3], XMLdsig [4] (enveloped-подпись), WS-Security [5] (detached-подпись);
- криптографические алгоритмы ГОСТ Р 34.10–2001 [6], ГОСТ Р 34.11–94 [7].

В зависимости от характера вызова проверка подписи может осуществляться по двум сценариям:

- только проверка – в этом случае проверяются все подписи под документом и итоговый результат содержит информацию по каждой из них;
- усиление подписи – проверяется и усиливается только одна подпись, вне зависимости от того, есть ли под документом еще подписи. В вызове должна присутствовать идентифицирующая усиливаемую подпись информация, данная информация должна быть предоставлена/согласована с заказчиком.

При наличии в CMS SignedData содержимого типа SignedData (вложенная подпись) производится проверка и этих данных. Поддержка заверяющих подписей (counterSignature) не требуется. Метод приведения xml к каноническому виду – xml-exc-c14n [8].

Сервис спроектирован с учетом того, что авторы проверяемых электронных документов принадлежат к изначально ограниченному и административно определяемому числу УЦ (набору издателей), сертификаты которых рассматриваются сервисом проверки как доверенные. Требований к корректному построению цепочки сертификатов в полном удовлетворении условий RFC 5280 в соответствии с методиками NIST PKITS [9] и [10] не предъявляется.

Проверка сертификатов авторов ЭП производится с учетом CRL, загружаемых сервисом архивирования CRL. К обработке принимаются только CRL и обновления к ним, непосредственно подписанные ключом того же доверенного издателя, что и проверяемый сертификат, либо, в случае indirectCRL, ключом специально выделенного для выпуска CRL сертификата, также непосредственно подписанным соответствующим издателем. В случае использования indirect-CRL сертификат, выделенный соответствующим издателем для выпуска CRL, должен устанавливаться в ПАК административными средствами, аналогично сертификату издателя.

В случае если для проверки передан блок XML-данных, поддерживаются:

- проверка непосредственно переданного XML, если входными аргументами не указано иное;
- проверка отдельного элемента переданного XML, определяемого по переданному в аргументах ID.

Результаты проверки содержат в виде XML всю информацию, находящуюся в информационной части сертификата автора проверяемой подписи.

В SVS присутствует поддержка проверки отсоединенных подписей, в этом случае исходные данные должны передаваться дополнительным параметром в запросе к сервису.

В зависимости от характера запроса SVS либо просто проверяет подпись под полученным документом, либо, в случае успешной проверки подписи и сертификата автора, проверяемые данные дополняются необходимыми атрибутами, с тем чтобы привести обрабатываемые данные, в зависимости от исходного формата, в соответствие спецификациям XAdES-C [11] или CAdES-C [12], для формата WS-Security усиление выполняется аналогично XadES-C.

Сервис формирования ЭП (SS)

SS оформлен как веб-сервис для доступа по HTTP через OSB. SS поддерживает:

- форматы подписи – CMS SignedData, XMLdsig (enveloped-подпись), XAdES-T, WS-Security (detached-подпись);
- криптографические алгоритмы ГОСТ Р 34.10–2001, ГОСТ Р 34.11–94.

SS как веб-сервис содержит функцию, предоставляющую потребителям (информационным системам) возможность выработки хэш-функции от произвольных бинарных данных.

Сервис архивирования CRL (CAS)

Назначение сервиса – предоставлять потребителям (компонентам ПАК) комплект из регулярного CRL и последнего обновления к нему, если технические средства конкретного УЦ поддерживают публикацию deltaCRL[1] от заданного издателя на заданную дату.

Сервис (CAS-1) спроектирован с учетом необходимости размещения ПАК в защищенном сегменте сети, не имеющем доступа к сети Интернет.

Компонент сервиса CAS, предназначенный для загрузки CRL и обновлений к ним из точек публикации (CAS-2), размещается в отдельном сегменте сети, откуда доступ в Интернет возможен, а коммуникация между CAS-2 и остальными компонентами ПАК осуществляется в офлайн-режиме посредством передачи файлов на отчуждаемых носителях или через TCP/IP-подключение.

Поддерживаемые протоколы доступа к точкам публикации CRL – http.

Точка публикации CRL должна определяться на основании соответствующего (стандартного, CDP или FreshestCRL соответственно для регулярных CRL и их обновлений) расширения проверяемого сертификата. В случае отсутствия такого расширения должна использоваться точка публикации CRL по умолчанию.

Загрузка регулярных CRL производится по следующему алгоритму, т.е. попытки загрузки должны начинаться:

- для отсутствующего CRL – немедленно;
- для очередного регулярного CRL – за некоторое фиксированное время до наступления даты, указанной в поле nextUpdate имеющегося CRL.

Подсистема администрирования

Подсистема предназначена для мониторинга и управления компонентами ПАК. Она обеспечивает мониторинг компонентов системы с автоматическим восстановлением работоспособности ПАК в случае программных сбоев и уведомлением администратора в случае необходимости, настройку ПАК на эталонный источник времени для протокола ntp [18]. Предоставляет средства управления списком доверенных издателей и параметрами сервиса архивирования CRL, в том числе:

- средства импорта/экспорта сертификатов доверенных издателей и соответствующих им CRL. Средства экспорта обеспечивают выгрузку данных как для одного, так и для нескольких или всех установленных издателей;
- возможность отметить определенного издателя как неактивного (в этом случае загрузка/обновление соответствующих CRL производиться не будет) либо полностью удалить издателя и все соответствующие ему CRL;
- возможность задания/изменения точки публикации CRL по умолчанию для определенного издателя;
- возможность задания упреждающего периода для загрузки очередного регулярного CRL;
- возможность принудительной загрузки/обновления CRL для одного, нескольких или всех активных издателей.

[1] Здесь и далее описание атрибутов и расширений сертификатов открытого ключа приводится из приказа ФСБ России № 795 [13] или на RFC 5280 [14], на которые есть ссылка из приказа ФСБ России. Следует также учитывать, что особенности представления отечественных криптографических алгоритмов в протоколах и форматах отражены в документах [15], [16] и [17].

Подсистема предоставляет средства управления сертификатами и ключами, используемыми для выработки штампов времени и формирования ЭП в SS. Установленные в системе контейнеры CSP должны быть защищены фиксированным предопределенным паролем.

Глава 2
Условия, необходимые для выполнения программы

Состав программных средств

Для развертывания ПАК может быть использован дистрибутив Альт Линукс 6.0 "Кентавр" для платформы x86-64, доступный для загрузки по адресу:

http://www.altlinux.ru/products/6th-platform/centaurus/

Данный дистрибутив будет использоваться в соответствии с лицензией производителя дистрибутива (ООО "Альт Линукс"):

http://www.altlinux.ru/products/license/

Также можно использовать дистрибутив CentOS 7.0.

В частности, на основании п. 2.2 данной лицензии используются компиляторы, загрузчики, препроцессоры, библиотеки, пакеты, сборки и т.п., входящие в состав данного дистрибутива.

Описание процедур установки и настройки компонентов ПАК "Jinn-Server" см. в документе "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство администратора".

Состав технических средств

Аппаратная платформа ПАК "Jinn-Server" реализована в виде двух промышленных системных блоков:

- Блок, содержащий программный модуль CAS-2, размещаемый в DMZ и имеющий выход в публичные телекоммуникационные сети. Специальных требований к аппаратной платформе не выдвигается. Для передачи данных модулю CAS-1 требуется USB-порт для отчуждаемого носителя.
- Блок, содержащий программные модули SS, SVS, CAS-1, подсистему администрирования, СКЗИ и возможность установки электронного замка "Соболь" с интерфейсом PCI-Express (уточняется при разработке). Аппаратная платформа для обеспечения требований по производительности должна быть построена на серверных чипсетах Intel и укомплектована серверным процессором семейства Intel Xeon 5000 или более современным, с количеством вычислительных ядер не менее 6 и тактовой частотой не менее 2,4 ГГц, а также оперативной памятью не менее 16 ГБ.

Аппаратные платформы должны иметь возможность подключения клавиатуры, монитора и компьютерной мыши непосредственно или через KVM (keyboard, video and mouse).

Электропитание должно осуществляться через устройство бесперебойного питания.

Резервное и архивное копирование информационных активов ПАК осуществляется на внешние USB-флеш-накопители общесистемными средствами. Правила и порядок выполнения операций копирования определяются эксплуатационной документацией прикладной системы.

Требования к персоналу

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы и гипертекстовых серверов.

Персонал должен быть аттестован на II квалификационную группу по электробезопасности (для работы с конторским оборудованием).

В перечень задач, выполняемых оператором, должны входить задачи эксплуатационного характера:

- оперативное управление ПАК средствами графического гипертекстового интерфейса подсистемы администрирования:
- задача контроля за статусом работоспособного состояния;
- актуализация списка поддерживаемых УЦ (в том числе и через обработку TSL-списков), а также точек распространения CRL и их обновлений;
- задача транспортировки информации между компонентами ПАК CAS-1 и CAS-2;
- задача ведения архивных копий информационных активов ПАК (хранилища СУБД, прикладные и системные журналы и т.д.).

В рамках своих задач оператор взаимодействует и с администратором системы, и с программистом.

Глава 3
Оперативная работа с ПАК "Jinn-Server"

Все основные компоненты ПАК "Jinn-Server" функционируют в автоматическом режиме, за исключением задач оперативного управления и актуализации списка УЦ и CRL; транспортировки информации между компонентами CAS-1 и CAS-2; задачи ведения архивных копий информационных активов ПАК.

Элементы оперативного управления ПАК "Jinn-Server"

Графический интерфейс

Элементы оперативного управления ПАК вынесены в специальную подсистему администрирования (ее краткое описание см. выше), взаимодействие оператора с которой осуществляется средствами штатного браузера через графический интерфейс, построенный с учетом свойств языка HTML. Со стороны сервера поддержку графического интерфейса выполняет гипертекстовый сервер.

Графический интерфейс предоставляет следующий функционал оператору.

В верхней части экрана расположена панель навигации с гиперссылками по разделам "Процессы", "Общие настройки", "Регистрация издателей", "Обработка TSL" и "Поиск издателей".

На рисунке 2 представлен примерный вид формы раздела "Процессы", показывающий основные показатели мониторинга процессов, такие как наименование, порт, сервер и состояние. Оператору следует контролировать показатель "состояние" в режиме "ЗАПУЩЕН", в противном случае привлекать иных специалистов с ролями "системный программист (администратор)" и/или "программист" для устранения нештатной ситуации и запуска процесса.

Процессы CAS

Процесс [0]	
Название:	CSM WEB ADMIN
Сервер:	tccs1.top-cross.lan
Порт:	80
Состояние:	ЗАПУЩЕН

Процесс [1]	
Название:	CRL Archive Daemon
Сервер:	tccs1.top-cross.lan
Порт:	11112
Состояние:	ЗАПУЩЕН

Процесс [2]	
Название:	PostgreSQL
Сервер:	tccs1.top-cross.lan
Сокет:	/tmp/.s.PGSQL.5432
Состояние:	ЗАПУЩЕН

Рис. 2. Примерный вид формы раздела "Процессы"

Следующая форма представлена на рисунке 3 и предназначена для оперативного изменения конфигурационного файла.

Рис. 3. Примерный вид формы раздела "Общие настройки"

Следующая форма, представленная на рисунке 4, предназначена для занесения в информационные активы ПАК "Jinn-Server" информации об издателях УЦ, подписи и сертификаты пользователей которых принимаются к обработке ПАК.

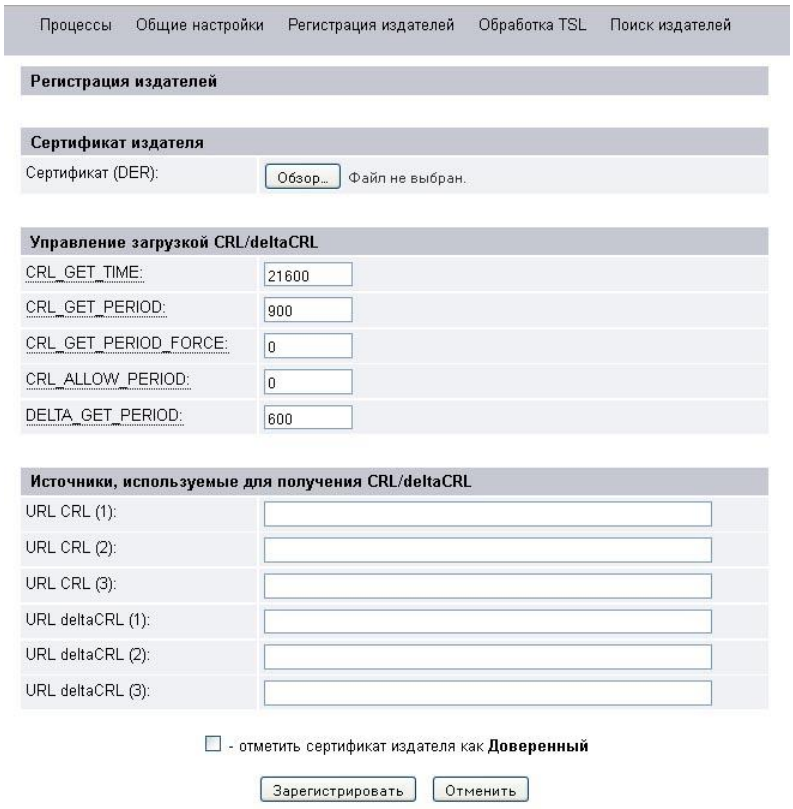

Рис. 4. Форма раздела "Регистрация издателей"

Представленная форма содержит три блока, первый – позволяет загрузить с локального компьютера в хранилище ПАК сертификат издателя в DER-кодировке. Второй блок – определяет временные характеристики обработки CRL, данные по умолчанию берутся из глобальных переменных конфигурационного файла формы "Общие настройки". Наведение курсора на переменную выводит на экран пояснение по работе с конкретной переменной.

Следующий раздел графического интерфейса позволяет выполнить поиск, визуализацию, выгрузку и удаление информационных объектов, связанных с издателями УЦ. На рисунке 5 представлена форма шаблона поиска. Следует обратить внимание, что поиск можно осуществлять отдельно по хранилищам для действительных сертификатов и сертификатов, размещенных в архиве.

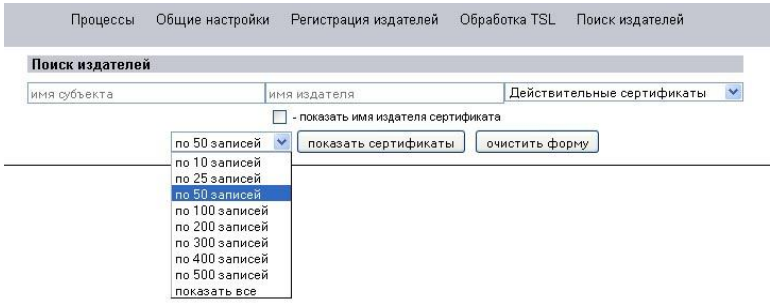

Рис. 5. Форма раздела "Поиск издателей"

Для детализации шаблона можно использовать поля для поиска в "Subject" сертификата по типу LIKE. Результатом поиска будет список (возможно, многостраничный), примерный вид которого представлен на рисунке 6.

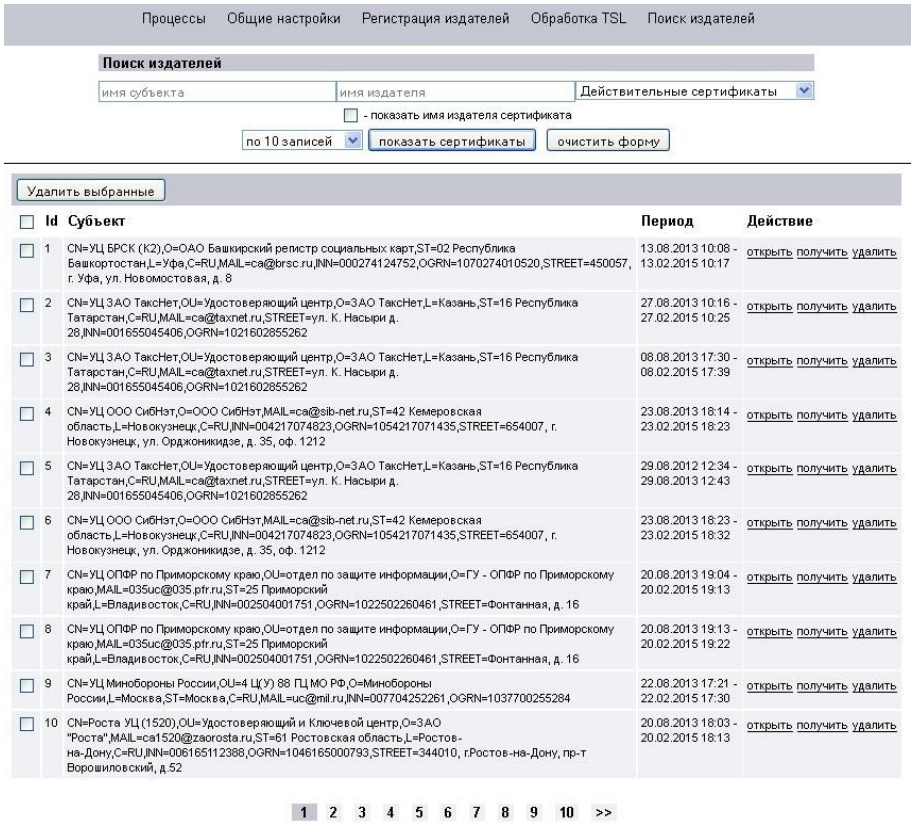

Рис. 6. Список найденных издателей, удовлетворяющих шаблону поиска

Полученный список позволяет выполнить примитивные операции с зарегистрированными сертификатами: открыть (детализировать информацию о сертификате издателя и связанную с ним информацию), получить (выгрузить из хранилища) сертификат издателя и удалить запись из хранилища о конкретном сертификате. Следует иметь в виду, что при удалении издателя уничтожается

ВСЯ сопутствующая информация и о сертификатах авторов CRL, если таковые были определены, и т.п.

При детализации информации о сертификате издателя внешний вид формы имеет примерно следующий вид, как показано на рисунке 7.

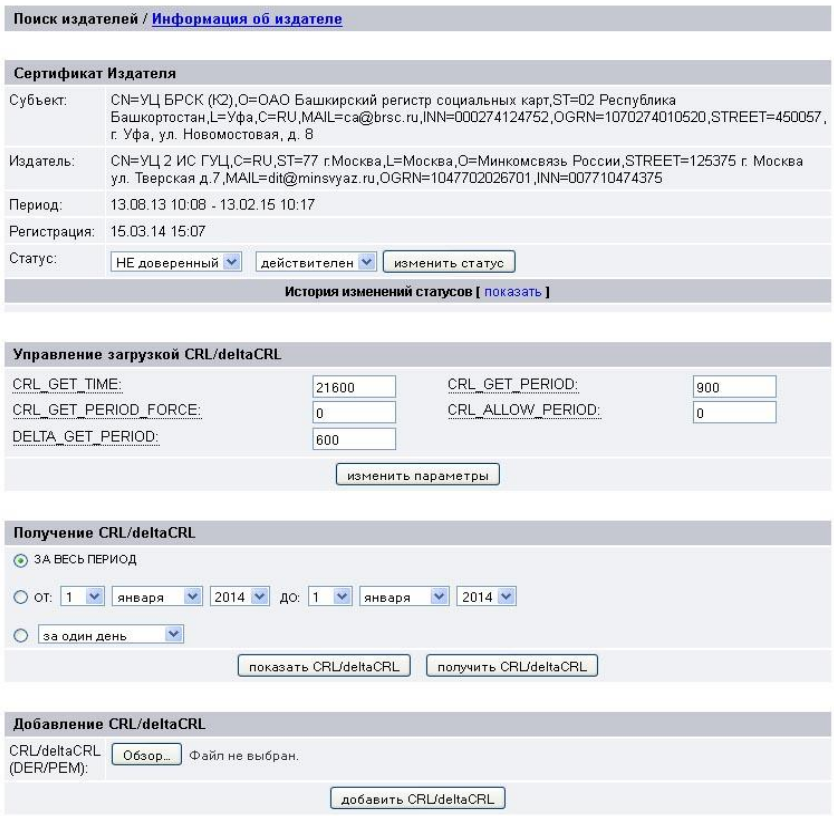

Рис. 7. Примерный вид формы детализации информации о сертификате издателя

На экране информация сгруппирована в несколько блоков:

- Информация о самом сертификате и возможность изменить его статус.
- История изменения статуса сертификата издателя.
- Параметры, определяющие режимы обработки CRL для данного сертификата издателя.
- Извлечение списков CRL (с возможностью определения диапазона выборки). Выгрузка осуществляется в один файл PEM-кодировки с разделителями между CRL.
- "Докладывание" в ручном режиме списка CRL или обновления.
- Корректировка источников CRL и обновлений, если таковые были ранее определены в ручном режиме либо извлечены автоматически из атрибутов CDP и/или FreshestCRL. Примерный вид экранной формы представлен на рисунке 8.

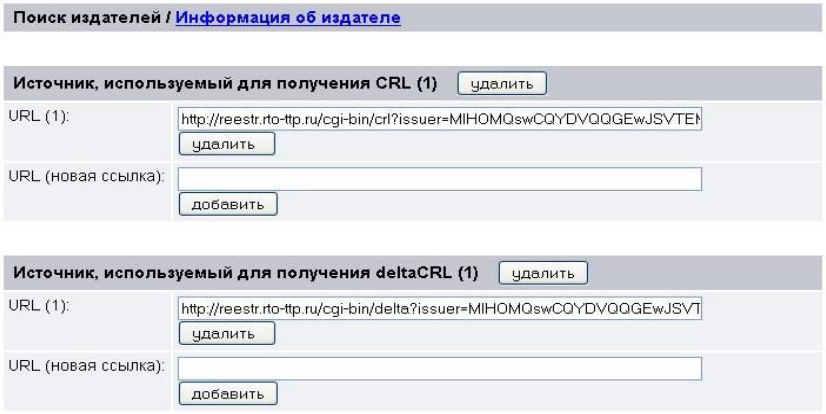

Рис. 8. Примерный вид формы управления источниками распространения CRL и обновлений

Для возврата в меню "Информация об издателе" можно воспользоваться гиперссылкой в верхней части экрана.

- Управление и регистрация самостоятельных авторов CRL, если таковые используются. На рисунке 9 представлен примерный вид такой формы.

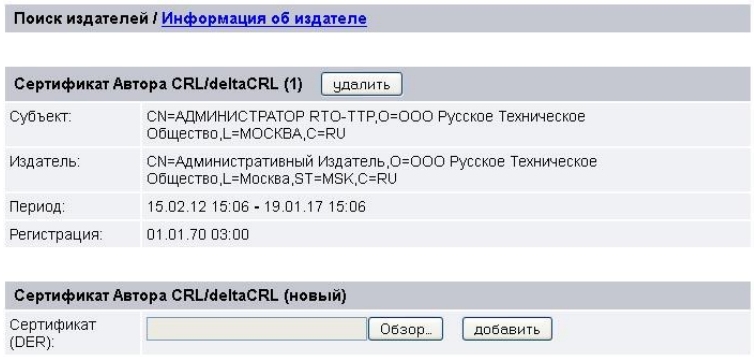

Рис. 9. Примерный вид формы управления сертификатами авторов CRL и обновлений, связанных с доменом конкретного издателя

Вкладка "Обработка TSL" предоставляет механизм управления загрузкой списков доверенных издателей и включает следующие функциональные возможности, представленные на рисунке 10.

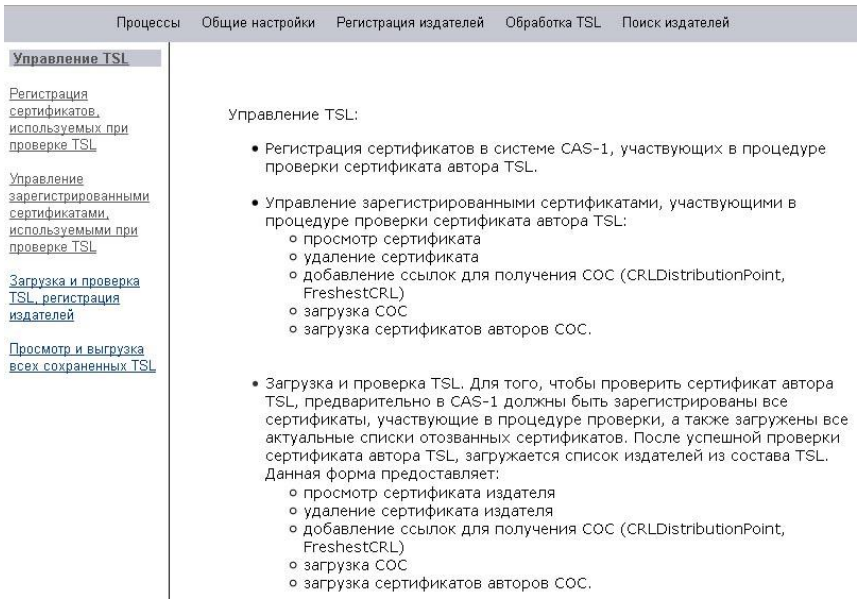

Рис. 10. Функции управления TSL

Графический интерфейс для регистрации сертификатов, участвующих в построении цепочки сертификатов для сертификата автора TSL, представлен на рисунке 11.

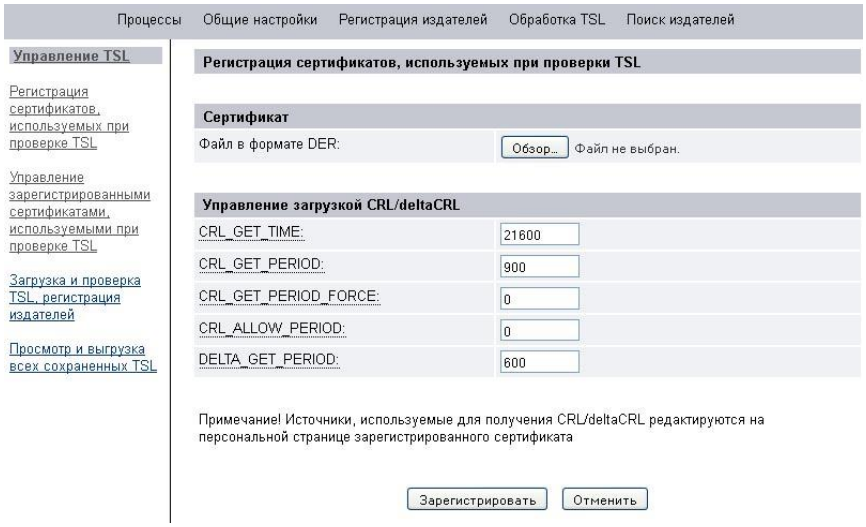

Рис. 11. Интерфейс регистрации сертификатов

Форма для управления зарегистрированными сертификатами представлена на рисунке 12.

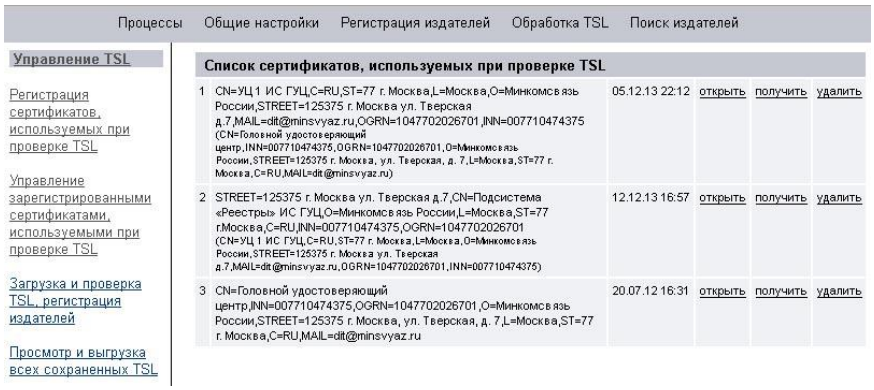

Рис. 12. Управление зарегистрированными сертификатами

Загрузка и проверка TSL, регистрация издателей из состава TSL представлены на рисунке 13.

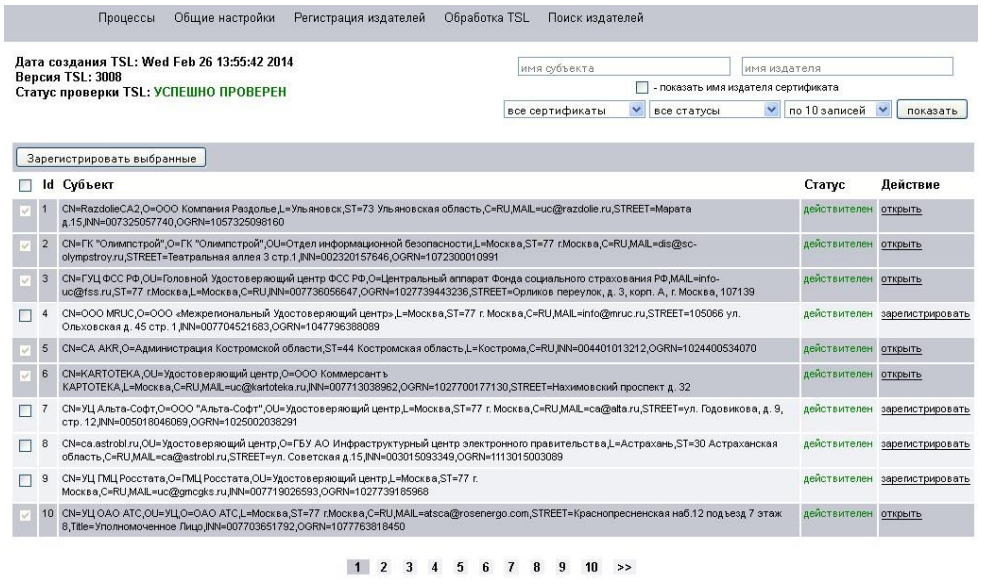

Рис. 13. Содержание TSL

На рисунке представлен примерный вид графического представления списка, темным цветом отмечены сертификаты, уже содержащиеся в базе издателей, и по таким сертификатам можно выполнить процедуру их детализации (функция "открыть"), более светлым цветом отмечены "новые", не содержащиеся в базе сертификаты издателей, но содержащиеся в TSL-списке, с предоставлением возможности оператору загрузить сертификат из списка в базу (функция "зарегистрировать").

Оператору предоставляется специальный интерфейс управления списками TSL – выборочный просмотр и выгрузка.

На рисунке 14 представлена поисковая форма в архиве списков.

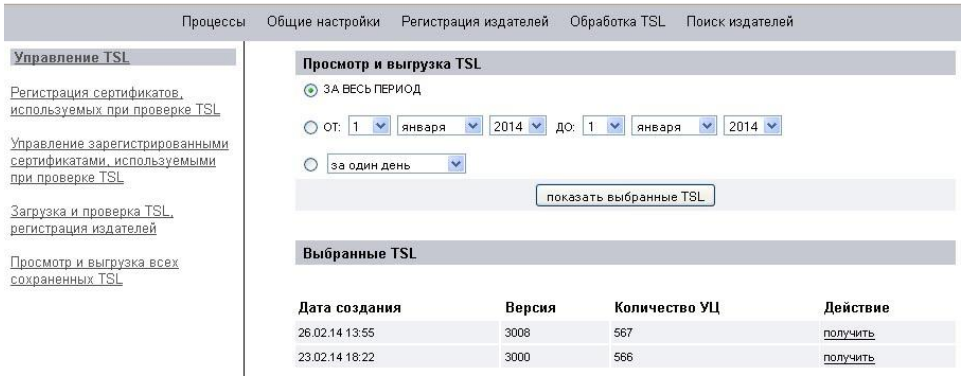

Рис. 14. Поисковая форма в архиве списков

Требуемый список можно выгрузить в виде файла, определив действие на форме "получить".

Консольный интерфейс

Помимо графического интерфейса, часть задач, стоящих перед оператором, решается средствами консоли для следующих процедур:

1. Анализ загруженности дискового пространства. Может использоваться команда df или другие схожие команды на усмотрение оператора. В случае занятости любого из разделов на файловой системе на 80% и выше необходимо принять соответствующие меры[2]. Процедура выполняется на компонентах CAS-1 и CAS-2.
2. Анализ загруженности оперативной памяти. Может использоваться команда top или другие схожие команды на усмотрение оператора. В случае использования оперативной памяти на 80% и выше необходимо принять соответствующие меры. Процедура выполняется на компонентах CAS-1 и CAS-2.
3. Анализ загруженности процессора(ов). Может использоваться команда top или другие схожие команды на усмотрение оператора. В случае использования процессора(ов) на 60% и выше необходимо принять соответствующие меры. Процедура выполняется на компонентах CAS-1 и CAS-2.
4. Проверка работоспособности базы данных PostgreSQL. Должна быть выполнена команда ps ax | grep postgres. Успешным результатом выполнения данной команды является вывод на консоль следующей информации:

```
 [pid1]  pts/2    S      [time1] /usr/bin/postgres -D
/var/opt/tccs/db

 [pid2] ?        Ss     [time2] postgres: writer
process

 [pid3] ?        Ss     [time3] postgres: wal writer
process
```

[2] Здесь и далее под "соответствующими мерами" подразумеваются действия обслуживающего персонала с различными ролевыми признаками, направленные на приведение показателей в указанный диапазон/состав.

```
 [pid4] ?        Ss     [time4] postgres: autovacuum
launcher process

 [pid5] ?        Ss     [time5] postgres: stats
collector process
```

В противном случае необходимо запустить исполняемый скрипт /opt/tccs/etc/init.d/psqld restart и повторить выполнение предыдущей команды. Если результат будет по-прежнему отрицательным, необходимо принять соответствующие меры.

Процедура транспортировки информации между компонентами CAS-1 и CAS-2

Одним из этапов проверки электронной подписи ПАК "Jinn-Server" является этап определения статуса сертификата автора подписи на момент проверки. Для решения этой задачи 63-ФЗ [1] предполагает использование реестров с отозванными сертификатами (списки отозванных сертификатов), актуальность и доступ к которым обязаны обеспечить аккредитованные УЦ. Технически реестры выполнены в виде информационных объектов доступа, расположенных в публичной сети Интернет, противодействие возможным атакам из которой не может обеспечить используемый класс защищенности ни самого СКЗИ, ни среды его функционирования. Для решения этой задачи модуль, отвечающий за архивирование и сбор списков отозванных сертификатов, был выполнен в виде двух компонентов, первый из которых расположен во внешнем сегменте сети и решает задачи сбора списков, а второй – предоставляет собранные списки процедурам проверки подписи. Обмен информацией между компонентами выполняется в регламентные промежутки времени на отчуждаемом носителе, тем самым компоненты выполняют свои функции, но не имеют технической связи как возможного канала внешней атаки.

Обмен информацией между составными частями сервиса архивирования CRL (CAS) выполняет оператор ПАК.

Перед тем как использовать отчуждаемый носитель, его необходимо инициализировать. Процедура инициализации состоит из создания на носителе пустого файла с названием ".crl".

Регламент обмена информацией между CAS-1 и CAS-2 состоит из следующих этапов, периодичность их выполнения зависит от общего регламента системы и влияет только на степень актуальности списков отозванных сертификатов:

1. При подключении носителя в USB-порт компонента CAS-1 оператор должен отслеживать процесс использования носителя через консоль. Успешным результатом использования носителя в CAS-1 является вывод следующей информации на консоль:

```
[ time1 ]  Монтирование внешнего носителя .. ВЫПОЛНЕНО

[ time2 ] Экспорт базы данных для CAS2 на внешний
носитель .. ВЫПОЛНЕНО

[ time3 ]  Импорт CRL/Delta с внешнего носителя в базу
данных CAS1 .. ВЫПОЛНЕНО

[ time4 ]  Работа с внешним носителем завершена
```

2. Далее оператор извлекает носитель из USB-порта, данная операция приводит к автоматическому размонтированию томов и сопровождается консольным сообщением вида:

```
[ time ]  Внешний носитель успешно размонтирован
```

3. Далее следует подключить отчуждаемый носитель в компонент CAS-2. Успешным результатом использования носителя будет вывод следующей информации на консоль:

```
[ time1 ]  Монтирование внешнего носителя .. ВЫПОЛНЕНО
```

```
[ time2 ]  Выгрузка CRL/Delta из CAS2 на внешний
носитель .. ВЫПОЛНЕНО

[ time3 ]  Импорт базы данных CAS1 в CAS2 .. ВЫПОЛНЕНО

[ time4 ]  Работа с внешним носителем завершена
```

4. Выполняется шаг №2.
5. После этого необходимо снова подключить отчуждаемый носитель в компонент CAS-1 и дождаться результата посредством консоли.
6. Выполняется шаг №2.

На этом шаге процесс обмена информацией между компонентами закончен. На время перерыва между циклами обмена отчуждаемый носитель должен находиться в состоянии "доверенное хранение", не допускающем модификацию содержимого на носителе.

ВАЖНО: В компонентах CAS-1, CAS-2 ЗАПРЕЩЕНО подключение и монтирование любых отчуждаемых носителей в ручном режиме (например, с помощью команды mount) в раздел /var/opt/tccs/cache на файловой системе. Подобные действия приведут к некорректной работе системы.

Ведение архивных копий прикладных информационных активов ПАК "Jinn-Server"

Для задач упрощения последующего аудита функционирования ПАК, а также минимизации времени восстановления штатного режима функционирования ПАК в обязанности оператора входит (может входить) задача ведения архивных копий журналов, а также наряду/совместно (взаимно дополняя персональные и групповые полномочия) с обслуживающим персоналом с ролевым признаком "программист" ведение архивных копий содержания таблиц и настроек СУБД. Более подробно см. соответствующий раздел документа "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство программиста".

Приложение

Сообщения

Компоненты ПАК "Jinn-Server" в своем составе содержат специальные модули, обеспечивающие активный мониторинг процессов и автоматический перезапуск в случае их "падения". Оповещение обслуживающего персонала осуществляется транспортом электронной почты на указанные в конфигурации адреса. Программа информирует по факту следующих событий:

- Процесс не запущен ("упал").
- Попытка запустить процесс автоматически.
- Результат процедуры автоматического перезапуска.
- Дневной отчет по перечню контролируемых процессов.

Настройка конфигурации активного мониторинга выполняется обслуживающим персоналом с ролью "программист" и описана в документе "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn-Server" версии 1.0. Руководство программиста".

Список используемых источников

1. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи". Принят Государственной Думой 25 марта 2011 года. Одобрен Советом Федерации 30 марта 2011 года.
2. RFC 2616, R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1", June 1999.
3. RFC 5652, R. Housley, "Cryptographic Message Syntax (CMS)", September 2009.
4. XML-DSig, XML-Signature Syntax and Processing. D. Eastlake, J. Reagle, and D. Solo. IETF Draft Standard/W3C Recommendation, August 2001. Available at http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.
5. WSS X509 Certificate Token Profile, OASIS Standard, 15 March 2004, Copyright © OASIS Open 2002, 2003, 2004. All Rights Reserved.
6. ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи. Издательство стандартов, 2001.
7. ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хэширования. Издательство стандартов, 1994.
8. XML-C14N, Canonical XML. J. Boyer. W3C Recommendation, March 2001. Available at http://www.w3.org/TR/2001/REC-xml-c14n-20010315 Available at http://www.ietf.org/rfc/rfc3076.txt.
9. Test Suite – "Public Key Interoperability Test Suite (PKITS) Certification Path Validation", Version 1.0, September 2, 2004.
10. Recommendation – D.A. Cooper, W.T. Polk, Draft Special Publication 800-XXX, "NIST Recommendation for X.509 Path Validation", Version 0.5, May 3, 2004.
11. ETSI TS 101 903, Technical Specification, "XML Advanced Electronic Signatures (XadES)" (2002-02).
12. RFC 5126, D. Pinkas, N. Pope, J. Ross, "CMS Advanced Electronic Signatures (CAdES)", March 2008.
13. Приказ ФСБ России от 27 декабря 2011 г. N 795 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ". Зарегистрировано в Минюсте РФ 27 января 2012 г., регистрационный N 23041.
14. RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.
15. RFC4490 Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS).

16. RFC4491 Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

17. draft-chudov-cryptopro-cpxmldsig-07 Using GOST 28147-89, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms for XML Security.

18. RFC 1305, David L. Mills, "Network Time Protocol (Version 3) Specification, Implementation and Analysis" March 1992.