КОД безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

Jinn-Server
Версия 1.3

Руководство пользователя

RU.88338853.501430.024 92

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

Оглавление

Введение

Данное руководство предназначено для пользователей, работающих с изделием "Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3" (далее — ПАК Jinn-Server, Jinn-Server, комплекс, ПАК). В руководстве содержатся сведения, необходимые для работы с графическим интерфейсом подсистемы администрирования и автоматизированным рабочим местом разбора конфликтных ситуаций ПАК Jinn-Server.

Дополнительные сведения по работе с ПАК Jinn-Server содержатся также в [**1**] и [**2**].

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://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
АРМ РКС	Автоматизированное рабочее место разбора конфликтных ситуаций
БД	База данных
ГУЦ	Головной удостоверяющий центр
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации. СКЗИ осуществляет криптографическое преобразование информации для обеспечения ее безопасности
СМЭВ	Система межведомственного электронного взаимодействия
СОС (CRL)	Список отозванных сертификатов (Certificate revocation list)
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр. УЦ в рамках своей деятельности осуществляет создание сертификатов ключей проверки ЭП, а также ведет реестр CRL
ЭД	Электронный документ
ЭП	Электронная подпись
API	Application Programming Interface — программный интерфейс приложения
CAdES	CMS Advanced Electronic Signatures (расширенная версия формата CMS) — формат ЭП
CAS	CRL Archiving Service — сервис, предназначенный для сбора и автоматического обновления списков отозванных сертификатов и обновлений к ним (deltaCRL) с целью последующего использования хранимых CRL другими компонентами Jinn-Server
CDP	CRL Distribution Point — точки распространения (публикации) CRL УЦ
CFV	Certificate Format Validation — составная часть сервиса SVS, предназначенная для проверки сертификатов авторов подписи на соответствие требованиям к квалифицированным сертификатам
CMS	Cryptographic Message Syntax (синтаксис криптографических сообщений) — формат ЭП
CSA	Conflict Service Audit — сервис разбора конфликтов
deltaCRL	Обновление к СОС, выпускаемое УЦ в интервале между выпусками СОС
DNS	Domain Name System — система доменных имен
HTML	HyperText Markup Language — язык гипертекстовой разметки
HTTP	HyperText Transfer Protocol — протокол передачи гипертекста
IP	Internet Protocol — межсетевой протокол
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
MTOM	Message Transmission Optimization Mechanism — механизм оптимизации передачи сообщений
NTP	Network Time Protocol — протокол сетевого времени
SNMP	Simple Network Management Protocol — протокол сетевого управления
SOAP	Simple Object Access Protocol (простой протокол доступа к объектам) — протокол обмена структурированными сообщениями в распределенной вычислительной среде
SS	SigningService — сервис, предназначенный для формирования ЭП
SVS	SignatureValidationService — сервис, предназначенный для проверки данных, подписанных ЭП, и усиления ЭП
TCP	Transmission Control Protocol — протокол управления передачей данных
TSL	Trusted Service List — список доверенных издателей (аккредитованных УЦ)
UDP	User Datagram Protocol — протокол пользовательских датаграмм
URL	Uniform Resource Locator — сетевой адрес ресурса
WebUI	Графический интерфейс подсистемы администрирования Jinn-Server
WS-Security (WSSec)	Web Services Security — формат ЭП блоков XML-данных

Термин	Определение
XAdES	XML Advanced Electronic Signatures (расширенная версия формата XMLDSig) — формат ЭП блоков XML-данных
XML	eXtensible Markup Language — расширяемый язык разметки
XMLDSig	XML Digital Signature — формат ЭП блоков XML-данных
XSLT	eXtensible Stylesheet Language Transformations — язык преобразования XML-документов

Глава 1
Общие сведения о ПАК Jinn-Server

Назначение, состав и структура ПАК Jinn-Server

ПАК Jinn-Server совместно с набором дополнительных программных средств предназначен для выполнения функции автоматической проверки и формирования ЭП документов с последующей сетевой выгрузкой результата криптографического преобразования во внешний сервис клиентской системы электронного документооборота, формирующей запросы на проверку и выработку ЭП к Jinn-Server.

Программное обеспечение Jinn-Server построено по модульному принципу и состоит из следующих веб-сервисов:

- сервис проверки ЭП (SVS — SignatureValidationService) — предназначен для проверки данных, подписанных ЭП, и усиления ЭП (в зависимости от параметров запроса), а также проверки сертификатов ЭП на действительность и соответствие требованиям к квалифицированным сертификатам;
- сервис формирования ЭП (SS — SigningService) — предназначен для выработки ЭП;
- сервис архивирования COC/CRL (CAS — CRLArchivingService) — предназначен для сбора 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);
- графический интерфейс подсистемы администрирования (WebUI, сервис ADMIN) — предназначен для мониторинга и конфигурации компонентов комплекса, а также для работы с сертификатами;
- сервис разбора конфликтов — предназначен для рассмотрения спорных ситуаций, возникающих при проверке ЭП, а также получения дополнительной информации по действительности сертификатов и ЭП на заданный момент времени. Данная информация используется в дальнейшем для урегулирования всех спорных юридических вопросов, связанных с особенностями PKI инфраструктуры.

На Рис. 1 представлена общая схема развертывания компонентов ПАК Jinn-Server (выделены светлым оттенком охры) и их взаимодействие с внешними информационными системами (выделены синим цветом).

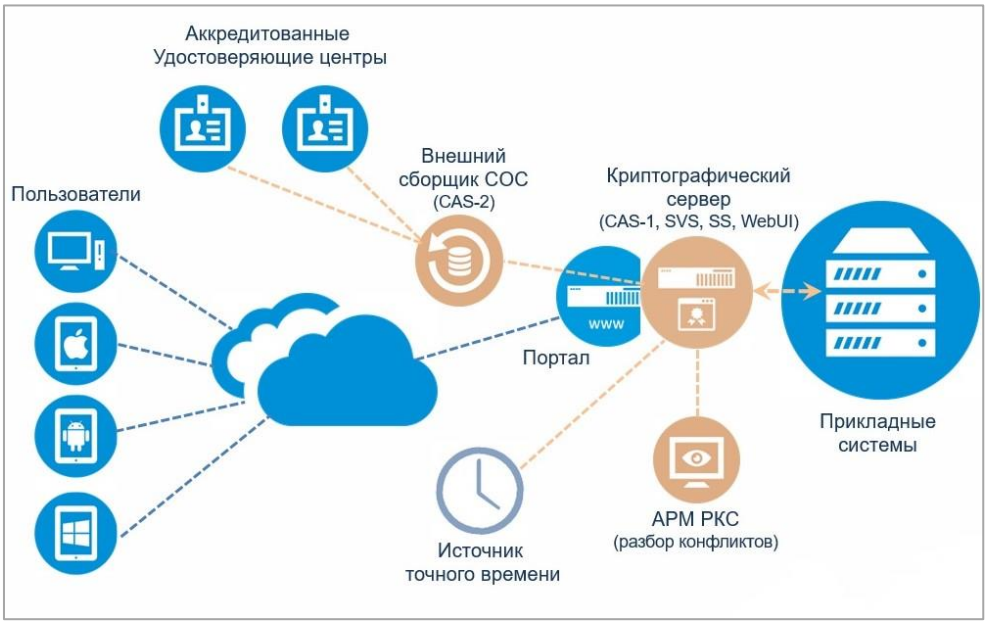


Рис. 1 Общая схема развертывания компонентов ПАК Jinn-Server

Аппаратная архитектура ПАК Jinn-Server состоит из следующих серверов и АРМ:

- криптографический сервер (сервер CAS–1) — сервер с развернутыми программными модулями CAS–1, SVS, SS, ADMIN и СКЗИ "КриптоПро CSP" 5.0;
- внешний сборщик COC (сервер CAS–2) — сервер с развернутым программным модулем CAS–2, размещаемый в DMZ и имеющий выход в открытые телекоммуникационные сети (интернет);
- АРМ РКС — наличие отдельного АРМ для развертывания сервиса разбора конфликтов опционально.

Серверы и АРМ РКС, входящие в состав ПАК Jinn-Server, функционируют под управлением дистрибутива ОС семейства Linux — CentOS 8.1 x64.

Для хранения обрабатываемой информации на серверах CAS–1 и CAS–2 развернута БД csm под управлением СУБД PostgreSQL.

Архив собранных CRL передается между серверами CAS–2 и CAS–1 по протоколу TCP или с использованием отчуждаемого носителя (флеш-накопителя).

Для формирования штампов времени ЭП и синхронизации компонентов комплекса в ПАК Jinn-Server предусмотрена возможность работы с внешними источниками точного времени по протоколу сетевого времени NTP.

Доступ к криптографическим функциям производится с использованием MicrosoftCryptoAPI для СКЗИ "КриптоПро CSP" 5.0 для платформы ОС семейства Linux.

ПАК Jinn-Server может совместно работать с сертифицированным средством защиты информации ПАК "Соболь" версий 3.0, 3.1, 3.2 и антивирусным ПО Kaspersky Endpoint Security для Linux.

Сервисы ПАК Jinn-Server

Сервис проверки ЭП

Сервис SVS поддерживает следующие форматы ЭП — CMS, CAdES-BES, CAdES-T, CAdES-C, CAdES-A, XMLDSig, XAdES-BES, XAdES-T, XAdES-C, XAdES-A, WSSec-BES, WSSec-T, WSSec-C, WSSec-A.

Обработка заверяющей подписи (ЭП с атрибутом counterSignature) в Jinn-Server не поддерживается.

Сервис SVS выполняет криптографические преобразования по ГОСТ — ЭП в соответствии с ГОСТ Р 34.10–2012 и ГОСТ Р 34.10–2001, хэш-функция в соответствии с ГОСТ Р 34.11–2012 и ГОСТ Р 34.11–94.

Доступ к сервису SVS осуществляется поверх протокола HTTP по порту 8080 через внешний SOAP-запрос.

Сервис SVS обрабатывает входящие запросы на проверку ЭП, проверку и усиление ЭП, проверку структуры сертификата и проверку действительности сертификата.

Структура запросов к сервису SVS приведена в [**2**].

Примечание. Для передачи данных (запрос — ответ) при взаимодействии с сервисом SVS поддерживается использование MTOM.

При запросе на проверку ЭП проверяются все ЭП подписанного документа и итоговый результат содержит информацию о каждой из них.

Сервис SVS поддерживает проверку отсоединенных подписей. В этом случае исходные данные должны передаваться дополнительным параметром в запросе.

При проверке блоков XML-данных сервис SVS обеспечивает проверку всего XML или проверку отдельного элемента, входящего в XML, определяемого по ID переданного в параметрах запроса.

Сервис SVS при проверке подписи в формате WS-Security поддерживает обработку значения атрибута "actor", переданного дополнительным параметром в запросе.

Запрос на проверку и усиление ЭП поддерживает указание конкретного формата усиления, и в случае успешной проверки подписи и сертификата автора прове-

ряемые данные дополняются необходимыми атрибутами так, чтобы привести обрабатываемые данные, в зависимости от исходного формата, в соответствие указанной спецификации — CAdES-T, CAdES-C, CAdES-A, XAdES-T, XAdES-C, XAdES-A. Для формата WS-Security усиление выполняется аналогично XAdES.

При запросе на проверку и усиление подписи блоков XML-данных проверяется и усиливается только одна ("внешняя" по отношению к остальным подписанным элементам, входящим в XML) подпись, определяемая по ID переданного в параметрах запроса, если документ или его части подписаны несколькими подписями.

В сервис SVS встроен сервис CFV, который осуществляет проверку структуры сертификатов на соответствие требованиям к квалифицированным сертификатам.

Подтверждение действительности сертификатов авторов ЭП производится сервисом SVS путем проверки отсутствия сведений об отзыве (приостановке действия) проверяемых сертификатов в CRL УЦ, 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 indirect CRL, 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 через подсистему администрирования, аналогично сертификату издателя.

Сервис SVS спроектирован с учетом того, что авторы проверяемых ЭП принадлежат к изначально ограниченному и административно определяемому числу УЦ (набору издателей), сертификаты которых рассматриваются сервисом проверки как доверенные.

Сервис формирования ЭП

Сервис SS формирует ЭП в следующих форматах — CMS, CAdES-BES, CAdES-T, CAdES-C, CAdES-A, XMLDSig, XAdES-BES, XAdES-T, XAdES-C, XAdES-A, WSSec-BES, WSSec-T, WSSec-C, WSSec-A.

Сервис SS выполняет криптографические преобразования по ГОСТ — ЭП в соответствии с ГОСТ Р 34.10–2012 и ГОСТ Р 34.10–2001, хэш-функция в соответствии с ГОСТ Р 34.11–2012 и ГОСТ Р 34.11–94.

Доступ к сервису SS осуществляется поверх протокола HTTP по порту 8080 через внешний SOAP-запрос.

Сервис SS обрабатывает входящие запросы на расчет хэша или формирование ЭП в соответствии с явно указанным в запросе стандартом.

Структура запросов к сервису SS приведена в [**2**].

Примечание. Для передачи данных (запрос — ответ) при взаимодействии с сервисом SS поддерживается использование MTOM. При использовании MTOM в запросе указывается, что должна быть сформирована откреплённая ЭП, ответ сервера содержит только ЭП.

Сервис SS поддерживает формирование отсоединенных подписей.

При подписании блоков XML-данных сервис SS обеспечивает подписание всего XML или подписание отдельного элемента, входящего в XML, определяемого по ID переданного в параметрах запроса.

Сервис SS при формировании подписи в формате WS-Security поддерживает обработку значения атрибута "actor", переданного дополнительным параметром в запросе.

Сервис SS поддерживает применение набора трансформов (правил нормализации XML-документов) — XPath, XSLT, SMEV3, при их объявлении в составе структуры SignedInfo при формировании подписи в формате XMLDSig и её расширенных версий (XAdES, WS-Security) для взаимодействия со СМЭВ.

При формировании подписи доступен выбор одного из ключевых контейнеров, принадлежащего только указанной в запросе подсистеме.

Сервис архивирования CRL

Сервис CAS предназначен для загрузки 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), что продиктовано необходимостью размещения криптографических сервисов Jinn-Server и СКЗИ в защищенном сегменте сети, не имеющем доступа к сети интернет.

Модуль CAS–2, предназначенный для загрузки CRL и обновлений к ним из точек публикации, размещается в отдельном сегменте сети, откуда доступ в интернет возможен, а коммуникация между модулями CAS–2 и CAS–1 осуществляется посредством передачи файлов на учтенных отчуждаемых носителях или по TCP-протоколу по каналу, где передача данных контролируется установленными средствами защиты от сетевых атак, сертифицированными ФСТЭК России.

На Рис. 2 представлена общая схема взаимодействия сервисов SVS, SS и модулей сервиса CAS с внешними системами и между собой.

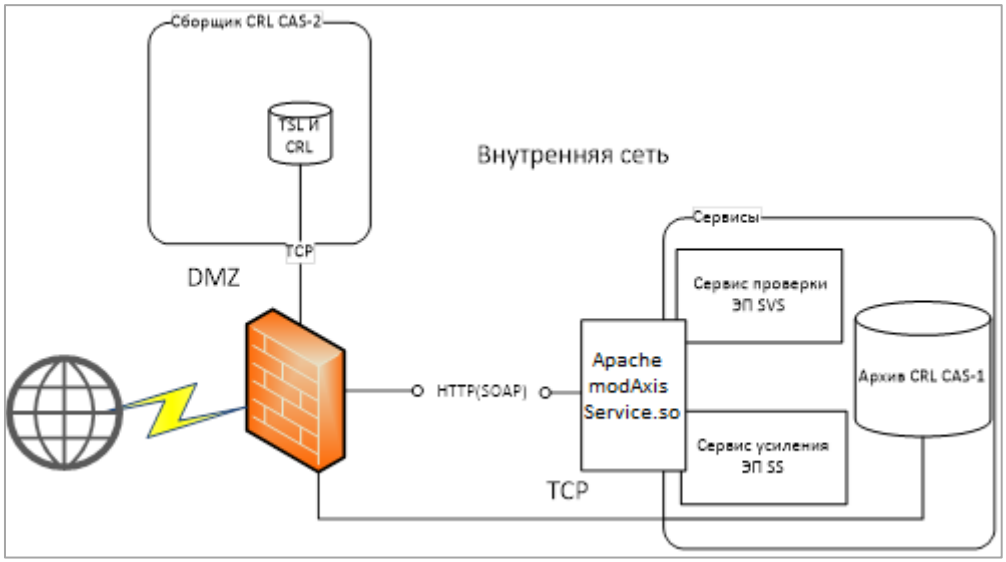


Рис. 2 Схема взаимодействия модулей сервиса CAS

Доступ к точкам публикации CRL осуществляется модулем CAS–2 по протоколу HTTP. Точки публикации CRL задаются при регистрации издателя через подсистему администрирования. Для доверенных УЦ из списка TSL точки публикации CRL определяются автоматически на основании соответствующего расширения (стандартного CDP или FreshestCRL — соответственно для регулярных CRL и их обновлений) сертификата УЦ. В случае отсутствия такого расширения у сертификата УЦ точки публикации его CRL задаются через подсистему администрирования.

Загрузка регулярных CRL из точек публикации осуществляется в автоматическом режиме через заданные в диспетчере расписаний интервалы времени. При этом для очередного регулярного CRL загрузка начинается за некоторое фиксированное время до наступления даты, указанной в поле nextUpdate имеющегося CRL.

Подсистема администрирования

Подсистема администрирования предоставляет графический интерфейс пользователю и обеспечивает мониторинг состояния сервисов ПАК Jinn-Server, а также возможность для изменения определенных конфигурационных настроек компонентов комплекса.

Подсистема администрирования предоставляет средства регистрации сертификатов и CRL УЦ — издателей ключевых контейнеров, использующихся сервисом SS при формировании ЭП и выработке штампов времени.

Подсистема администрирования предоставляет средства регистрации доверенных УЦ из списка TSL, что необходимо для функционирования сервисов проверки ЭП и разбора конфликтов.

Подсистема администрирования предоставляет средства управления сертификатами и CRL зарегистрированных УЦ:

- импорт/экспорт сертификатов УЦ и соответствующих им CRL. Средства импорта обеспечивают выгрузку данных для зарегистрированных издателей;
- возможность отметить сертификат определенного издателя как неактивный (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 для определенного издателя;
- возможность задания упреждающего периода для загрузки очередного регулярного CRL;
- возможность принудительной загрузки/обновления CRL для одного, нескольких или всех активных издателей.

Подсистема администрирования предоставляет средства проверки формата сертификатов на соответствие требованиям к квалифицированным сертификатам.

Сервис разбора конфликтов

Сервис разбора конфликтов предоставляет графический интерфейс пользователю и предназначен для рассмотрения следующих спорных ситуаций, в случае признания ЭП недействительной:

- оспаривание действительности ЭП документа путем проверки ЭП, определения даты ЭП, проверки подписи штампа времени (при наличии) и действительности цепочки сертификатов на момент подписи или на заданный пользователем момент времени;
- оспаривание действительности сертификата ключа проверки электронной подписи с помощью выстраивания цепочки сертификатов и проверки их действительности на момент времени, указанный в штампе времени, или на заданный пользователем момент времени.

Сервис разбора конфликтов формирует отчет о результатах проверки ЭП.

Глава 2
Условия функционирования ПАК Jinn-Server

Требования к программным средствам

ОС

Серверы CAS–1, CAS–2 и АРМ РКС, входящие в состав ПАК Jinn-Server, функционируют под управлением дистрибутива ОС семейства Linux — CentOS 8.1.

Также на основании лицензии производителя дистрибутива ОС используются компиляторы, загрузчики, препроцессоры, библиотеки, пакеты, сборки и т. п., входящие в состав дистрибутива.

СУБД

Для хранения обрабатываемой информации на серверах CAS–1 и CAS–2 развернута БД csm под управлением СУБД PostgreSQL.

Установка СУБД PostgreSQL и создание структуры БД csm осуществляется в процессе установки ПО Jinn-Server.

СКЗИ

Для формирования и проверки ЭП в ПАК Jinn-Server используется сертифицированное ФСБ России СКЗИ (вплоть до класса КС2 включительно, в части защиты информации, не содержащей сведений, составляющих государственную тайну) "КриптоПро CSP" 5.0 для платформы ОС семейства Linux производства компании "КРИПТО-ПРО".

ПАК Jinn-Server (класс защиты КС2) функционирует совместно с сертифицированным ФСБ России изделием "Программно-аппаратный комплекс "Соболь" версии 3.0/3.1/3.2 (далее — ПАК "Соболь").

Порты, используемые ПАК Jinn-Server

Порты, используемые ПАК Jinn-Server, приведены в таблице 1. Должен быть настроен доступ к указанным портам при конфигурации внешних средств защиты, таких как пакетные фильтры, межсетевые экраны и т.п.

Табл. 1 Порты, используемые ПАК Jinn-Server

Компонент	Порт	Характеристика сервиса
Сервер CAS–1	TCP_80	Гипертекстовый интерфейс управления и администрирования CAS–1
	TCP_8080	Транспортный протокол HTTP, обслуживающий запросы к сервисам формирования и проверки ЭП
	TCP_11112	CRL Archiving Daemon
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу
Сервер CAS–2	TCP_11113	Сборщик СОС
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу

Компонент	Порт	Характеристика сервиса
АРМ РКС	TCP_8083	Гипертекстовый интерфейс управления и администрирования АРМ РКС (доступ к интерфейсу проверки ЭП документов и отчетам о результатах проверки ЭП)
	TCP_8080	Транспортный протокол HTTP, обслуживающий запросы к сервису разбора конфликтов
	UDP_161, UDP_162	Службы SNMP
	TCP_22	SSH для удаленного доступа
	UDP_53 (исходящее соединение)	Доступ к DNS-серверу

Веб-обозреватель

Для работы графического интерфейса подсистемы администрирования используются следующие веб-обозреватели:

- Google Chrome 86;
- Mozilla Firefox 81.

Требования к аппаратным средствам

Сервер CAS–1

Сервер CAS–1 должен соответствовать следующим аппаратным требованиям:

- процессор Intel® Xeon 5000 (и выше) с количеством ядер не менее 6 и тактовой частотой не менее 2,4 ГГц;
- оперативная память не менее 64 ГБ;
- свободное дисковое пространство не менее 20 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;
- интерфейс USB 2.0;
- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

Сервер CAS–2

Сервер CAS–2 должен соответствовать следующим аппаратным требованиям:

- процессор Intel® семейства x86 (или совместимый) в соответствии с требованиями ОС, установленной на сервер;
- оперативная память не менее 16 ГБ;
- свободное дисковое пространство не менее 10 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;
- интерфейс USB 2.0;
- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

АРМ РКС

АРМ РКС должно соответствовать следующим аппаратным требованиям:

- процессор Intel® семейства x86 (или совместимый) в соответствии с требованиями ОС, установленной на АРМ;
- оперативная память не менее 2 ГБ;
- свободное дисковое пространство не менее 10 ГБ;
- сетевой интерфейс Ethernet 10/100/1000 Мбит/с;
- интерфейс USB 2.0;

- интерфейс PCI-E — для установки платы ПАК "Соболь" (наличие данного интерфейса опционально и зависит от варианта исполнения ПАК Jinn-Server);
- привод DVD/CD-ROM.

Требования к персоналу

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

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

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

- оперативная работа с ПАК средствами графического гипертекстового интерфейса подсистемы администрирования;
- контроль за статусом работоспособного состояния сервисов ПАК;
- актуализация списка поддерживаемых УЦ (в том числе и через обработку TSL-списков), а также точек распространения CRL и их обновлений;
- передача информации между серверами CAS–2 и CAS–1;
- работа с АРМ РКС.

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

Глава 3
Эксплуатация ПАК Jinn-Server

Графический интерфейс подсистемы администрирования

Для доступа к графическому интерфейсу подсистемы администрирования оператору необходимо в адресной строке веб-обозревателя ввести имя хоста или IP-адрес сервера CAS–1:

```
http://имя_хоста_или_IP-адрес_сервера_CAS-1
```

В окне веб-обозревателя появится окно "Вход". Необходимо пройти аутентификацию — ввести имя пользователя, пароль и нажать кнопку "Вход".

Примечание. Имя пользователя и пароль задает администратор ПАК Jinn-Server.

В окне веб-обозревателя появится веб-страница "Процессы системы" (загружается по умолчанию). В левом верхнем углу находится кнопка вызова меню ☰.

Главное меню подсистемы администрирования включает в себя следующие пункты:

Пункт меню	Назначение
Процессы	Отображение основных показателей мониторинга процессов (сервисов Jinn-Server)
Издатели	Регистрация УЦ, выдавших сертификаты ключевых контейнеров, зарегистрированных в ПАК Jinn-Server
Управление TSL	Регистрация сертификатов, используемых при проверке списка TSL, выгрузка, загрузка и проверка файла списка TSL
Политики проверки ЭП	Управление политиками проверки ЭП
Реестр СКЗИ	Управление перечнем средств защиты информации
Проверка сертификата	Проверка формата сертификата
Общие настройки	Изменение конфигурационного файла csm.conf сервера CAS–1
Лицензионное соглашение	Отображение лицензионного соглашения

Процессы

На Рис. 3 представлен вид страницы "Процессы системы", отображающей основные показатели мониторинга процессов (сервисов Jinn-Server) — статус, наименование, сервер, сокет и порт. Оператору следует контролировать показатель процесса "Статус" в режиме "Запущен", а при переходе процесса в состояние "Остановлен" привлекать иных специалистов с ролями "системный программист (администратор)" и/или "программист" для устранения нештатной ситуации и запуска остановленного процесса.

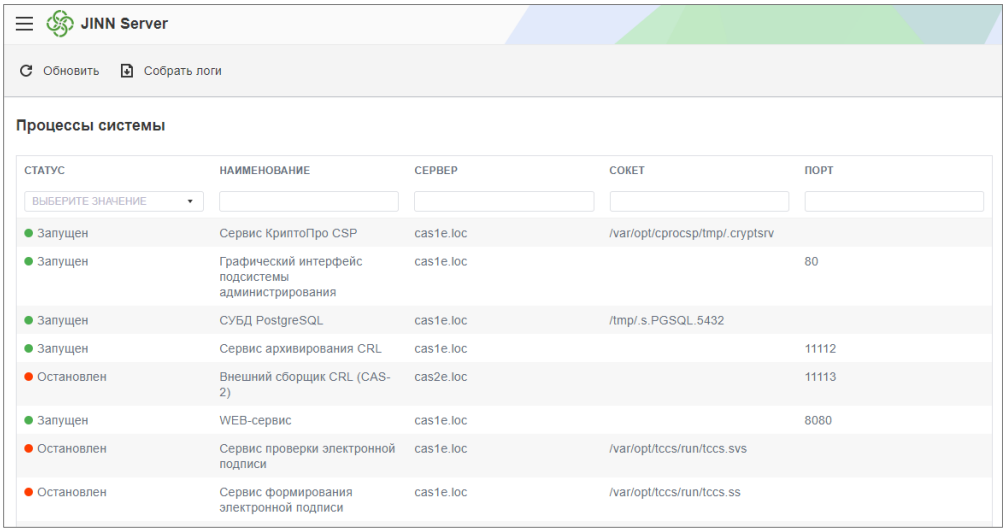


Рис. 3 Страница "Процессы системы"

Страница "Процессы системы" позволяет оператору:

- обновить страницу, нажав соответствующую кнопку;
- скачать лог-файлы о работе сервисов формирования и проверки электронной подписи, нажав кнопку "Собрать логи" и сохранив архив лог-файлов в выбранное место.

Примечание. Архив содержит лог-файлы о частичной работе сервиса проверки электронной подписи.

Издатели

На Рис. 4 представлен вид страницы "Издатели". На данной странице отображаются зарегистрированные сертификаты издателей и их параметры — субъект, издатель, дата начала, дата окончания и статус.

Примечание. Сроки действия сертификатов и CRL отображаются в формате UTC+0.

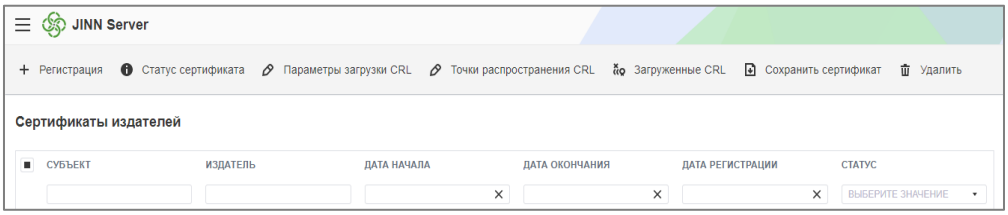


Рис. 4 Страница "Издатели"

На странице "Издатели" располагаются следующие кнопки:

Название кнопки	Назначение
Регистрация	Регистрация издателя с помощью загрузки с локального компьютера в БД csm ПАК Jinn-Server сертификат УЦ (издателя) в DER-кодировке (см. ниже)
Статус сертификата	Изменение статуса сертификата, просмотр истории изменений статусов (см. стр. 18)
Параметры загрузки CRL	Редактирование параметров загрузки CRL/deltaCRL, определение временных характеристик обработки. По умолчанию значения берутся из глобальных переменных конфигурационного файла csm.conf, доступного для редактирования на странице "Общие настройки" (см. стр. Параметры загрузки CRL18)
Точки распространения CRL	Добавление или редактирование точек распространения CRL, необходимых для получения списков CRL/deltaCRL регистрируемого УЦ (см. стр. 18)
Загруженные CRL	Добавление списков CRL/deltaCRL и сохранение их на локальный компьютер (см. стр. 19)
Сохранить сертификат	Сохранение сертификата на локальный компьютер в DER-кодировке (см. стр. 19)
Удалить	Удаление сертификата издателя (см. стр. 19)

Фильтрация сертификатов издателей выполняется по их параметрам — субъект, издатель, дата начала и дата окончания.

Регистрация издателя

Для регистрации издателя:

1. Откройте главное меню, выберите пункт "Издатели".

   Откроется страница "Сертификаты издателей".
2. Нажмите кнопку "Регистрация".

   Откроется страница "Регистрация издателя" (см. Рис. 5).

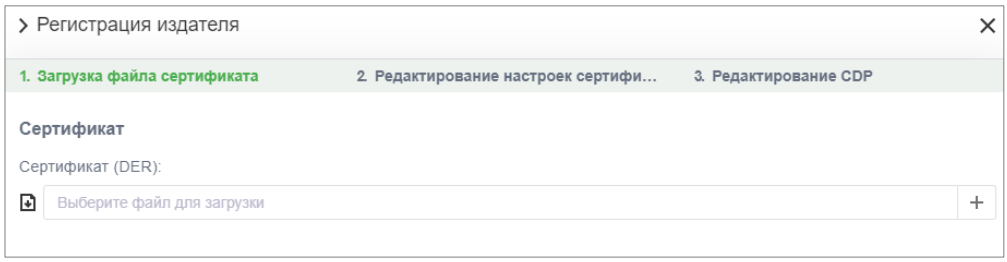


Рис. 5 Страница "Регистрация издателя"

3. Нажмите кнопку [+].

   На экране появится стандартный диалог выбора файла.

4. Укажите файл загружаемого сертификата в DER-кодировке и нажмите кнопку "Открыть".
5. Нажмите кнопку "Вперед" в правом нижнем углу.

   Откроется страница "Редактирование настроек сертификата".

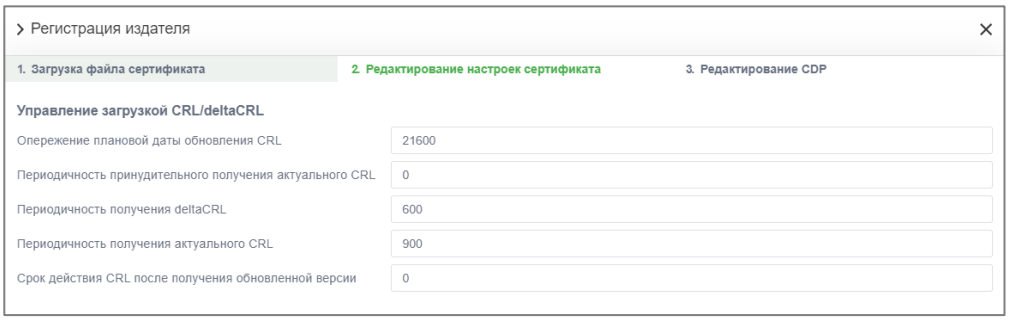


Рис. 6 Страница "Редактирование настроек сертификата"

6. При необходимости откорректируйте настройки сертификата и нажмите кнопку "Вперед" в правом нижнем углу.

   Откроется страница "Редактирование CDP".

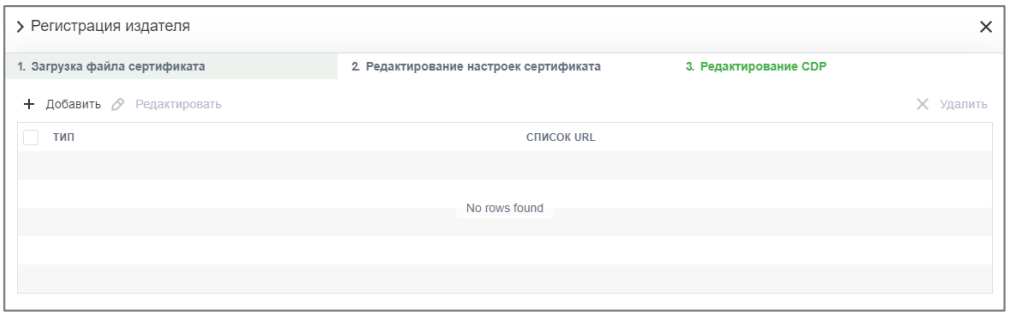


Рис. 7 Страница "Редактирование CDP"

7. При необходимости добавьте источник CRL следующим образом:
   - Нажмите кнопку "Добавить".
   - На открывшейся странице в поле URL укажите адрес источника CRL.
   - Для ввода еще одного адреса источника CRL нажмите кнопку "Добавить".

     Появится пустое поле URL, введите в него адрес источника CRL.

     Повторите для всех источников CRL.
   - Нажмите кнопку "Сохранить".
8. Нажмите кнопку "Готово" в правом нижнем углу.

   Сертификат появится в списке сертификатов издателей.

Статус сертификата

Для изменения статуса сертификата:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Статус сертификата".
   Откроется страница "Статус сертификата".

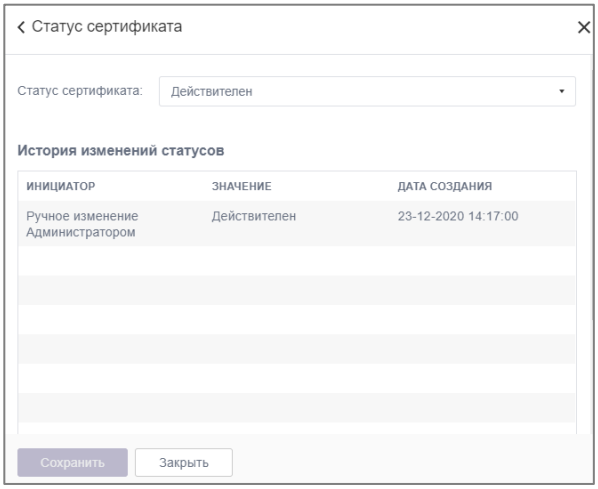


Рис. 8 Страница "Статус сертификата"

3. Выберите необходимый статус сертификата из выпадающего меню и нажмите кнопку "Сохранить".

Параметры загрузки CRL

Для редактирования параметров загрузки CRL/deltaCRL:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Параметры загрузки CRL".
   Откроется страница "Управление загрузкой CRL/deltaCRL".
3. Откорректируйте необходимые параметры и нажмите кнопку "Сохранить".

Точки распространения CRL

Для добавления точки распространения CRL:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Точки распространения CRL ".
   Откроется страница "Источники, используемые для получения CRL/deltaCRL" (см. Рис. 9).

Рис. 9 Страница "Источники, используемые для получения CRL/deltaCRL"

3. Нажмите кнопку "Добавить".
   Откроется страница "Параметры источника CRL".

4. В поле URL введите адрес источника.
5. Для ввода еще одного адреса источника CRL нажмите кнопку "Добавить".
   Появится пустое поле URL, введите в него адрес источника CRL.
   Повторите для всех источников CRL.
6. Нажмите кнопку "Сохранить".

Примечание. Для редактирования источника выберите источник и нажмите кнопку "Редактировать". Внесите нужные корректировки и нажмите кнопку "Сохранить".

Загруженные CRL

Для добавления списка CRL/deltaCRL:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Загруженные CRL".
   Откроется страница "Список CRL/deltaCRL" (см. Рис. 10).
3. Нажмите кнопку "Добавить".
   На экране появится стандартный диалог выбора файла.
4. Выберите нужный файл и нажмите кнопку "Открыть".
   Добавленный список отобразится на странице "Список CRL/deltaCRL".

Для сохранения списка CRL/deltaCRL на локальный компьютер:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Загруженные CRL".
   Откроется страница "Список CRL/deltaCRL" (см. Рис. 10).

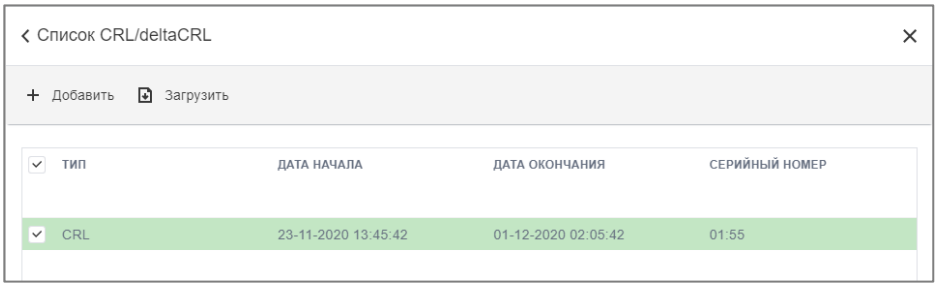


Рис. 10 Страница "Список CRL/deltaCRL"

3. Выберите нужный список CRL/deltaCRL и нажмите кнопку "Загрузить".
   На экране появится стандартный диалог сохранения файла.
4. Укажите место сохранения файла и нажмите кнопку "Сохранить".

Сохранение и удаление сертификата издателя

Для сохранения сертификата издателя на локальный компьютер:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите нужный сертификат и нажмите кнопку "Загрузить сертификат".
   На экране появится стандартный диалог сохранения файла.
3. Укажите место сохранения файла сертификата и нажмите кнопку "Сохранить".

Для удаления сертификата издателя:

1. Откройте главное меню, выберите пункт "Издатели".
   Откроется страница "Сертификаты издателей".
2. Выберите один или несколько сертификатов и нажмите кнопку "Удалить".
3. Подтвердите удаление выбранных сертификатов, нажав кнопку "Да".

Управление TSL

На Рис. 11 представлен вид страницы "Управление TSL". Данная страница содержит следующие вкладки:

Название вкладки	Назначение
Управление TSL	Получение текущего TSL (см. ниже)
Управление сертификатами	Просмотр, скачивание и удаление сертификатов, необходимых для проверки TSL (см. стр. 21Параметры загрузки CRL)
Регистрация сертификатов	Загрузка сертификатов, необходимых для проверки TSL (см. стр. 22)
Загрузка и проверка TSL	Просмотр сертификатов TSL. Доступна фильтрация по следующим критериям: • имя (поля "Имя субъекта" и "Имя издателя"); • сертификат (все, новые, зарегистрированные, ошибочные, неприменимые записи); • статус сертификата (все, приостановленные, прекращенные, действительные, аннулированные, неизвестные). Ручная регистрация сертификатов доверенных издателей в случае, если автоматическая регистрация издателей отключена (см. стр. 22)
Выгрузка TSL	Просмотр и выгрузка всех сохраненных TSL (см. стр. 23)

Внимание! Запрещается редактировать свойства сертификатов издателей во вкладке "Управление TSL" главного меню.

Примечание. Сроки действия сертификатов и CRL отображаются в формате UTC+0.

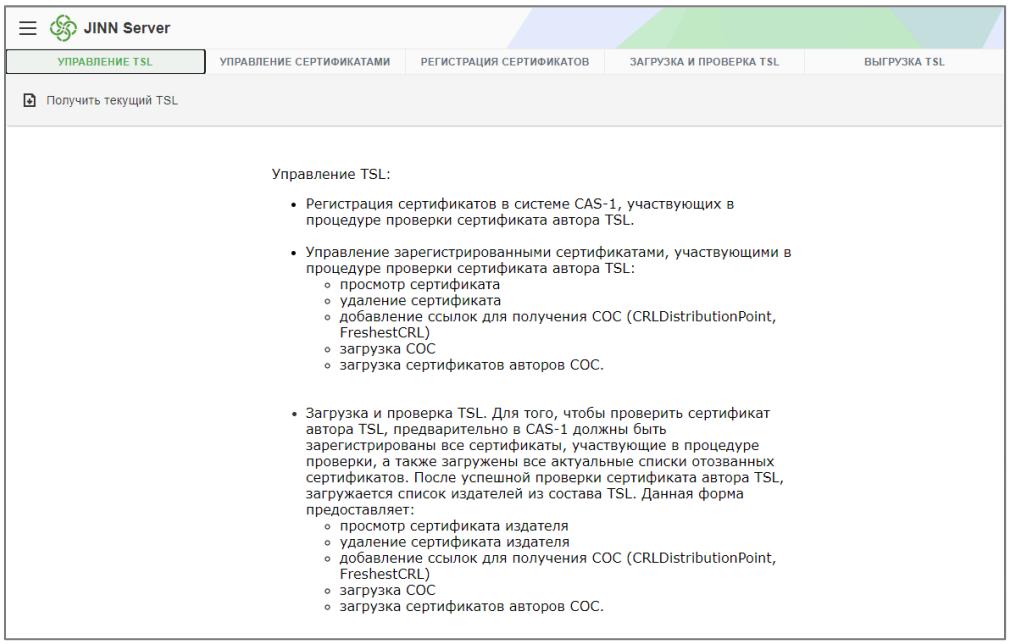


Рис. 11 Страница "Управление TSL"

Получение списка TSL

Актуальный список TSL оператор может выгрузить на странице "Управление TSL" или скачать по адресу — https://e-trust.gosuslugi.ru/#/portal/accreditation/accreditedcalist.

Для выгрузки текущего списка TSL на странице "Управление TSL":

1. Откройте главное меню, выберите пункт "Управление TSL".

   Откроется страница "Управление TSL".
2. Нажмите кнопку "Получить текущий TSL".

   На экране появится стандартный диалог сохранения файла.

3. Сохраните файл текущего списка TSL в выбранном месте.

Управление сертификатами

На Рис. 12 представлен вид вкладки "Управление сертификатами". На данной вкладке отображается список сертификатов, используемых при проверке TSL.

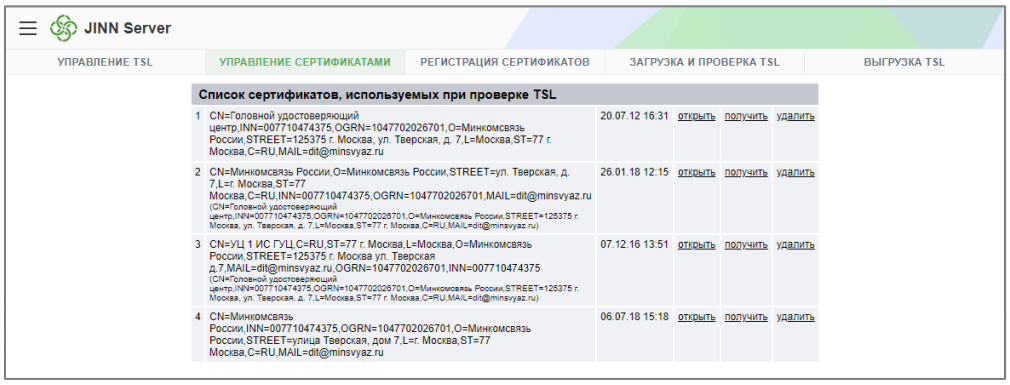


Рис. 12 Вкладка "Управление сертификатами"

Оператор может выполнить следующие действия с зарегистрированными сертификатами при нажатии на соответствующую ссылку:

- "открыть" — просмотреть детализированную информацию о сертификате;
- "получить" — выгрузить из БД Jinn-Server сертификат в виде файла (например, для проверки формата сертификата);
- "удалить".

При нажатии на ссылку "открыть" будет выполнен переход на форму просмотра детализированной информации о сертификате, вид которой представлен на Рис. 13.

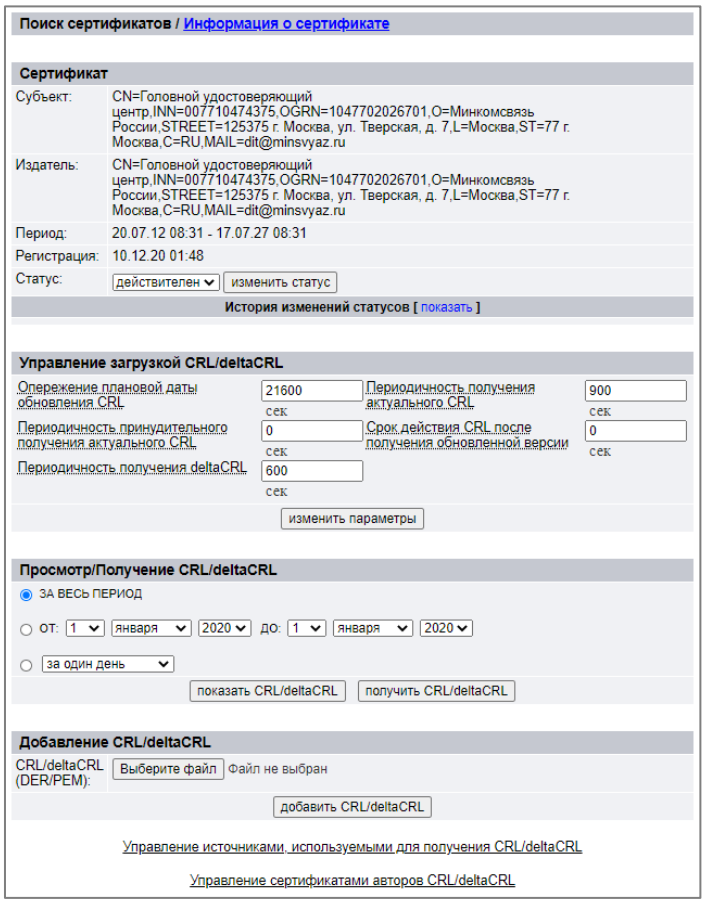


Рис. 13 Форма детализированной информации о сертификате

Регистрация сертификатов

На Рис. 14Рис. 12 представлен вид вкладки "Регистрация сертификатов". Данная вкладка позволяет регистрировать сертификаты, используемые при проверке списка TSL, и построить цепочку от сертификата ГУЦ до сертификата автора подписи под TSL (см. стр. Сертификаты, используемые при проверке TSL27).

Внимание! Сертификаты, используемые для проверки списка TSL, необходимо зарегистрировать дважды, один раз используя страницу "Издатели" (см. стр. 16) с указанием URL точек распространения CRL, и вторично, на странице "Управление TSL", выбрав кнопку "Регистрация", НЕ ДОБАВЛЯЯ URL точек распространения CRL.

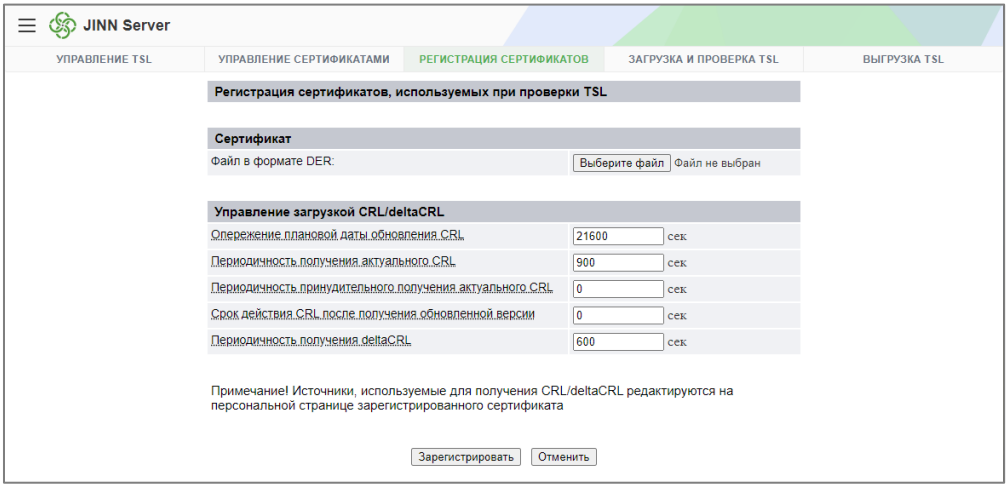


Рис. 14 Вкладка "Регистрация сертификатов"

Для регистрации сертификата, используемого при проверке TSL:

1. Откройте главное меню, выберите пункт "Управление TSL | Регистрация сертификатов".
2. Нажмите кнопку "Выберите файл" в блоке "Сертификат" (см. Рис. 14).

   На экране появится стандартный диалог выбора файла.
3. Выберите необходимый файл сертификата в формате DER (см. стр. Сертификаты, используемые при проверке TSL27) и нажмите кнопку "Открыть".
4. Нажмите кнопку "Зарегистрировать".

Загрузка и проверка TSL

Для загрузки и проверки списка доверенных издателей оператору необходимо выбрать вкладку "Загрузка и проверка TSL". При успешной проверке сертификата автора подписи под TSL загружается список сертификатов издателей из состава TSL, представленный на Рис. 15.

Примечание. Перед выполнением процедуры загрузки и проверки TSL должна быть зарегистрирована вся цепочка сертификатов, участвующих в проверке, а также добавлены списки CRL для зарегистрированных УЦ.

Если на сервере CAS–1 была установлена некорректная лицензия или она отсутствует, процедура загрузки и проверки TSL завершится ошибкой. Описание действий по установке лицензии приведено в [1].

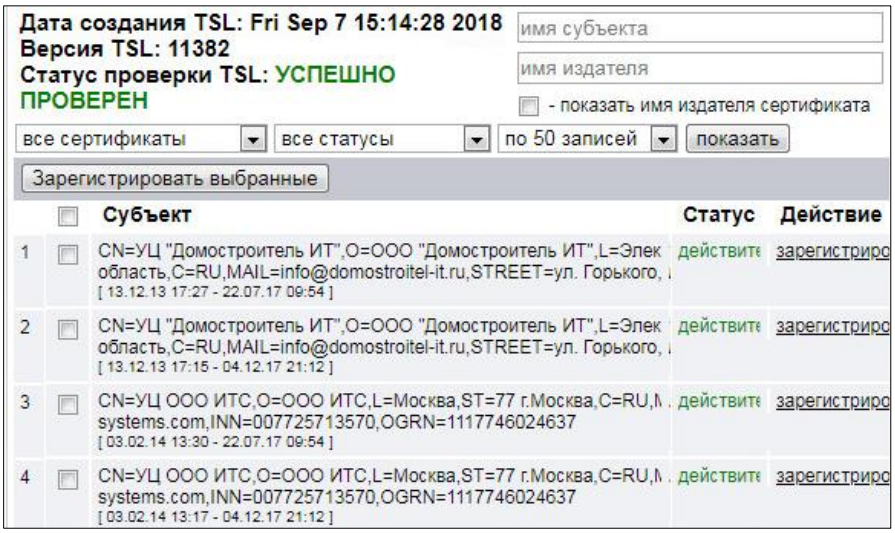


Рис. 15 Список сертификатов УЦ TSL

Для регистрации сертификатов УЦ из списка TSL оператору необходимо установить флаг "Субъект" для выделения всех записей незарегистрированных УЦ (если требуется выделить не всех, а один или несколько УЦ из отображенных на странице, то следует устанавливать флаги напротив соответствующих записей), после чего нажать кнопку "Зарегистрировать выбранные".

Выгрузка TSL

На Рис. 16 представлен вид вкладки "Выгрузка TSL". Для просмотра списков TSL за выбранный период оператору необходимо выбрать вкладку "Выгрузка TSL", задать необходимый период и нажать кнопку "показать выбранные TSL". Для сохранения выбранного списка TSL необходимо нажать ссылку "получить" и сохранить файл.

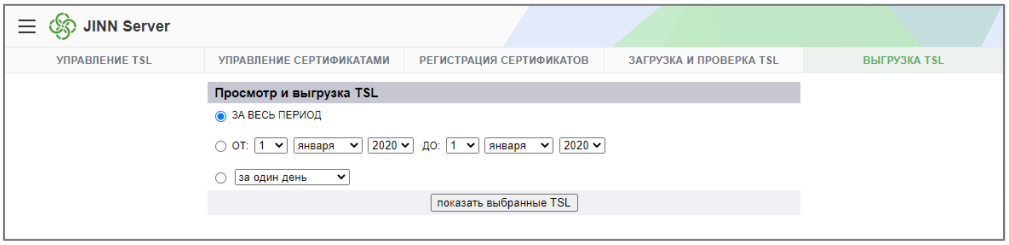


Рис. 16 Вкладка "Выгрузка TSL"

Политики проверки ЭП

На Рис. 17 представлен вид страницы "Управление политиками обработки ЭП", предназначенной для создания и управления политиками обработки ЭП.

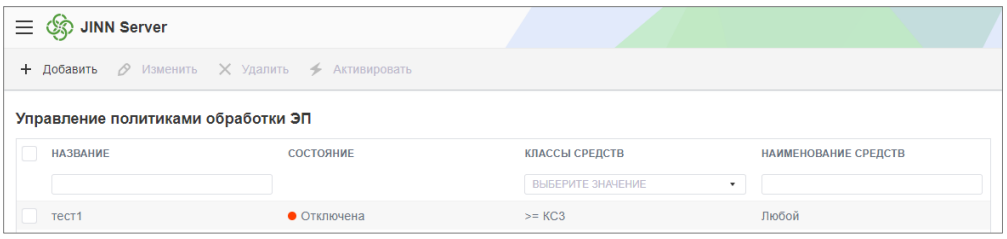


Рис. 17 Страница "Управление политиками обработки ЭП"

Страница "Управление политиками обработки ЭП" позволяет оператору:

- создать политику проверки ЭП;
- изменить или удалить существующую политику;
- активировать или деактивировать политику. Только одна политика проверки ЭП может иметь статус "Активна";

Примечание. Ключевые контейнеры, подходящие под действие правила активной политики, должны быть первыми в списке ключевых контейнеров, прошедших регистрацию в ПАК Jinn-Server (см. [1]), для корректного запуска сервисов.

- выполнять поиск политики по ее параметрам — название, классы средств, наименование средств.

Для создания политики обработки ЭП:

1. Откройте главное меню, выберите пункт "Политики проверки ЭП".

   Откроется страница "Управление политиками обработки ЭП".

2. Нажмите кнопку "Добавить".

   Откроется страница "Создание политики обработки ЭП" (см. Рис. 18).

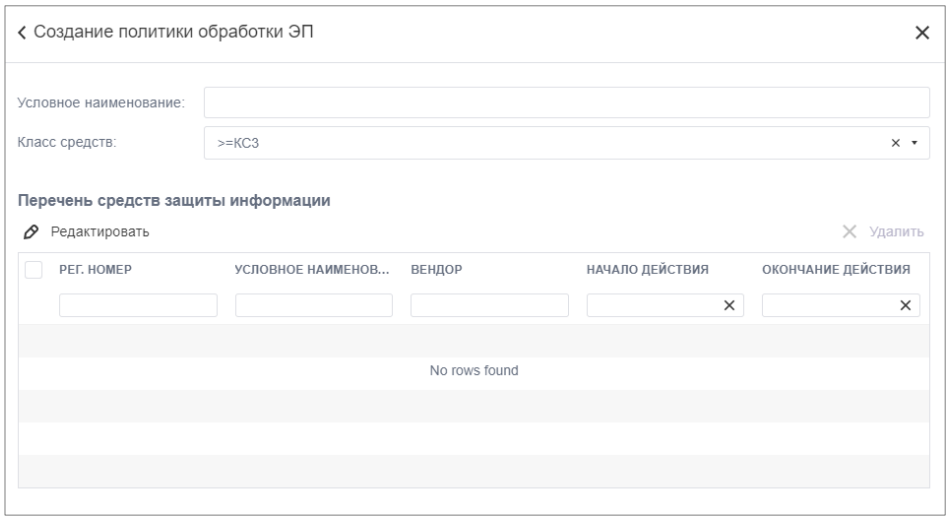


Рис. 18 Страница "Создание политики обработки ЭП"

3. В поле "Условное наименование" введите название политики.
4. При необходимости выберите в выпадающем меню нужный класс средств УЦ из следующих значений:
   - = КС1 (строго КС1);
   - ≥ КС1 (не менее КС1);
   - = КС2 (строго КС2);
   - ≥ КС2 (не менее КС2);
   - = КС3 (строго КС3);
   - ≥ КС2 (не менее КС3)
   - = КВ1 (строго КВ1);
   - ≥ КВ1 (не менее КВ1);
   - = КВ2 (строго КВ2);
   - ≥ КВ2 (не менее КВ2);
   - = КА1 (строго КА1).

   Для выбора значения "Нет КС" нажмите кнопку × в поле "Класс средств".
5. При необходимости выберите СКЗИ из перечня средств защиты информации.

Примечание. Если не выбрано ни одно СКЗИ, то под действие правила попадает любое из них.

6. Нажмите кнопку "Сохранить".

   На странице "Управление политиками обработки ЭП" отобразится созданная политика.

Для редактирования политики обработки ЭП:

1. Откройте главное меню, выберите пункт "Политики проверки ЭП".
   Откроется страница "Управление политиками обработки ЭП".
2. Выберите нужную политику и нажмите кнопку "Изменить".
   Откроется страница "Изменение политики обработки ЭП".
3. Внесите необходимые изменения и нажмите кнопку "Сохранить".

Для смены статуса политики обработки ЭП:

1. Откройте главное меню, выберите пункт "Политики проверки ЭП".
   Откроется страница "Управление политиками обработки ЭП".
2. Выберите нужную политику и нажмите кнопку "Активировать" или "Деактивировать".
3. Подтвердите изменение активности выбранной политики, нажав кнопку "Да".

Внимание! При смене статуса политики выполняется перезагрузка всех сервисов (альтернативное решение — перезагрузка сервиса tccs.svs администратором).

Политика станет активной и начнет применяться после завершения перезагрузки. Ориентировочно процесс занимает около 1 минуты.

Рекомендуется изменять статус политики обработки ЭП не чаще одного раза в минуту.

Для удаления политики обработки ЭП:

1. Откройте главное меню, выберите пункт "Политики проверки ЭП".
   Откроется страница "Управление политиками обработки ЭП".
2. Выберите нужную политику и нажмите кнопку "Удалить".
3. Подтвердите удаление выбранной политики, нажав кнопку "Да".

Примечание. Удалить активированную политику невозможно. Перед удалением смените статус политики, нажав кнопку "Деактивировать".

Реестр СКЗИ

На Рис. 19 представлен вид страницы "Перечень средств защиты информации", предназначенной для управления перечнем средств защиты информации.

Примечание. Сроки действия СКЗИ вводятся и отображаются в локальном формате времени, выставленном на устройстве пользователя.

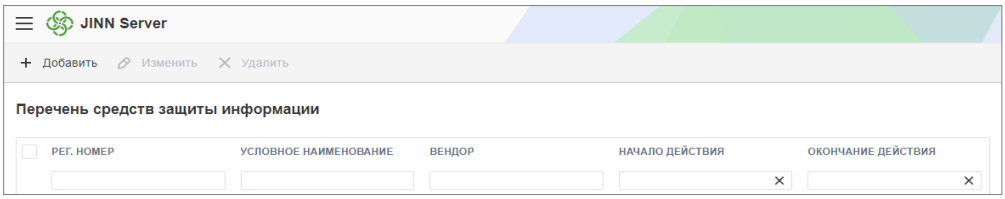


Рис. 19 Страница "Перечень средств защиты информации"

Страница "Перечень средств защиты информации" позволяет оператору:

- добавить СКЗИ;
- изменить или удалить из перечня СКЗИ;
- выполнять поиск СКЗИ по параметрам — регистрационный номер, условное наименование, вендор, начало и окончание действия.

Внимание! При добавлении, удалении или изменении параметров СКЗИ выполняется перезагрузка всех сервисов. Изменения вступят в силу после завершения перезагрузки, ориентировочно процесс занимает около 1 минуты.

Для добавления СКЗИ в перечень средств защиты информации:

1. Откройте главное меню, выберите пункт "Реестр СКЗИ".
   Откроется страница "Перечень средств защиты информации".

2. Нажмите кнопку "Добавить".
   Откроется страница "Создание СКЗИ" (см. Рис. 20).

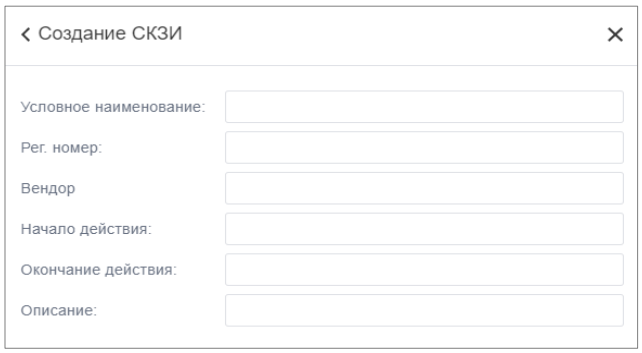


Рис. 20 Страница "Создание СКЗИ"

3. Заполните поля на странице и нажмите кнопку "Сохранить".

Для редактирования параметров СКЗИ:

1. Откройте главное меню, выберите пункт "Реестр СКЗИ".
   Откроется страница "Перечень средств защиты информации".
2. Выберите нужное СКЗИ и нажмите кнопку "Изменить".
   Откроется страница "Изменение СКЗИ".
3. Внесите необходимые изменения и нажмите кнопку "Сохранить".

Примечание. Для оперативного внесения изменений в параметры СКЗИ, входящих в активную политику, необходимо изменить ее статус на "Отключена", затем вновь назначить активной (см. стр. 25).

Для удаления СКЗИ из перечня средств защиты информации:

1. Откройте главное меню, выберите пункт "Реестр СКЗИ".
   Откроется страница "Перечень средств защиты информации".
2. Выберите нужное СКЗИ и нажмите кнопку "Удалить".
3. Подтвердите удаление выбранной политики, нажав кнопку "Да".

Примечание. СКЗИ будет удалено во всех политиках проверки ЭП.

Проверка сертификата

На Рис. 21 представлен вид страницы "Проверка формата сертификата", предназначенной для проверки сертификата на соответствие требованиям к формату:

- проверка декодирования сертификата;
- проверка на наличие неизвестных путей/неверных значений (ANY_BROKEN);
- проверка на удовлетворение правилам для разных типов собственников на основе приказа ФСБ России № 795 от 27 декабря 2011 г.

Рис. 21 Страница "Проверка формата сертификата"

Для проверки формата сертификата:

1. Откройте главное меню, выберите пункт "Проверка сертификата".

   Откроется страница "Проверка формата сертификата".
2. Выберите тип субъекта.
3. Нажмите кнопку "Выберите файл".

   На экране появится стандартный диалог выбора файла.
4. Укажите файл сертификата в формате DER для проверки.
5. Нажмите кнопку "Проверить сертификат".

   На экране отобразится отчет о проверке формата сертификата.

Общие настройки

На Рис. 22 представлен вид страницы "Общие настройки", предназначенной для оперативного изменения конфигурационного файла csm.conf сервера CAS–1.

Настройку конфигурационного файла должны производить специалисты с ролями "системный программист (администратор)" и/или "программист".

Описание параметров конфигурационного файла csm.conf приведено в [**1**].

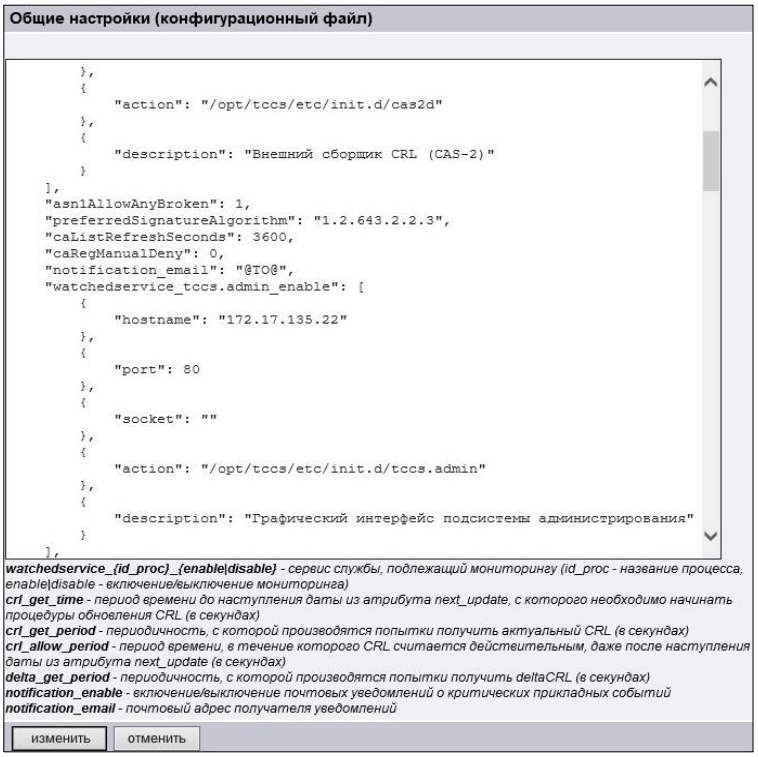


Рис. 22 Страница "Общие настройки"

Сертификаты, используемые при проверке TSL

В общем случае цепочка сертификатов, используемых при проверке TSL, состоит из следующих сертификатов:

- сертификат автора подписи под TSL;
- сертификат УЦ (издателя сертификата автора подписи под TSL), выданного ГУЦ;
- сертификат ГУЦ.

Сертификат автора подписи под TSL

Для регистрации сертификата автора подписи под TSL в кодировке DER оператору необходимо выполнить процедуры, приведенные ниже.

Для получения сертификата автора подписи под TSL:

1. Откройте список TSL в редакторе (Notepad++) и скопируйте фрагмент, заключенный внутри тега <X509Certificate> (см. Рис. 23).

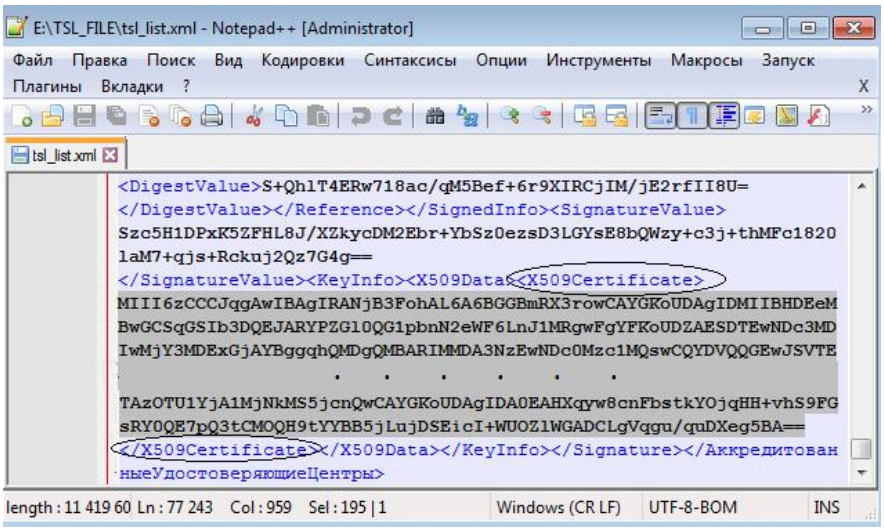


Рис. 23 Данные сертификата автора подписи под TSL

2. Сохраните скопированный фрагмент в файле с расширением ".cer" (например, под именем CertificateTSL.cer).

Полученный сертификат автора подписи под TSL сохранен в кодировке Base64. Для регистрации данного сертификата в Jinn-Server оператору необходимо преобразовать формат файла сертификата в кодировку DER.

Для преобразования формата файла сертификата автора подписи под TSL:

1. Двойным щелчком мыши откройте файл сертификата автора подписи под TSL.
2. Перейдите на вкладку "Состав" и нажмите кнопку "Копировать в файл".

   На экране появится окно мастера экспорта сертификатов.
3. Нажмите кнопку "Далее".

   На экране появится окно выбора формата файла сертификата.
4. Выберите сохранение файла в кодировке DER (см. Рис. 24) и нажмите кнопку "Далее".

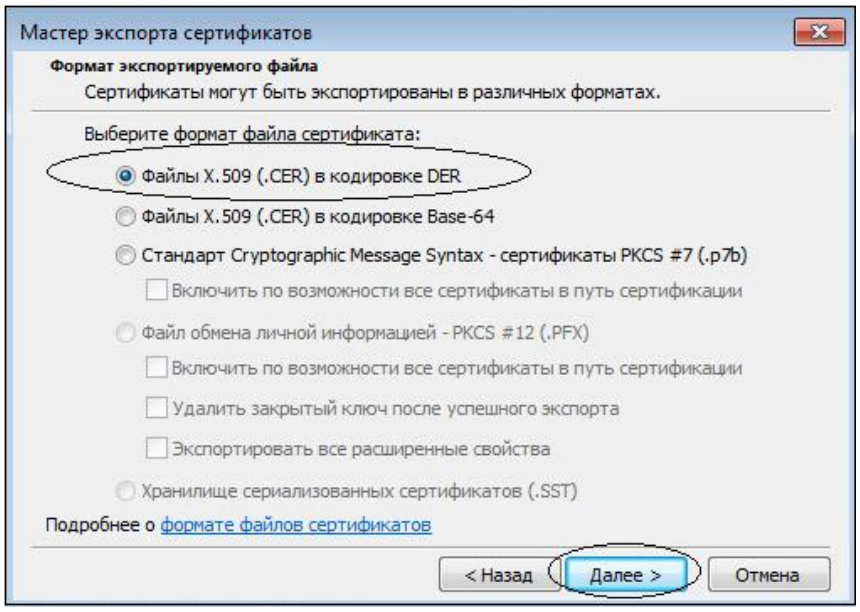


Рис. 24 Выбор кодировки сохранения сертификата

5. Укажите место сохранения файла сертификата в кодировке DER.
6. Нажмите кнопку "Далее" и затем кнопку "Готово", завершая работу мастера экспорта сертификатов.

После чего оператору необходимо зарегистрировать сертификат автора подписи под TSL (в кодировке DER) на странице "Издатели" (см. стр. 16) с указанием URL точек распространения CRL и затем вторично, на странице "Управление TSL" (см. стр. 22), без указания URL точек распространения CRL.

Сертификат УЦ (издателя сертификата автора подписи под TSL)

Для регистрации сертификата УЦ (издателя сертификата автора подписи под TSL) оператору необходимо выполнить процедуру, приведенную ниже.

Для получения сертификата УЦ (издателя сертификата автора подписи под TSL):

1. Двойным щелчком мыши откройте файл сертификата автора подписи под TSL.
2. Перейдите на вкладку "Состав", выделите поле "Идентификатор ключа центра сертификатов" и зафиксируйте значение идентификатора ключа, как показано на Рис. 25.

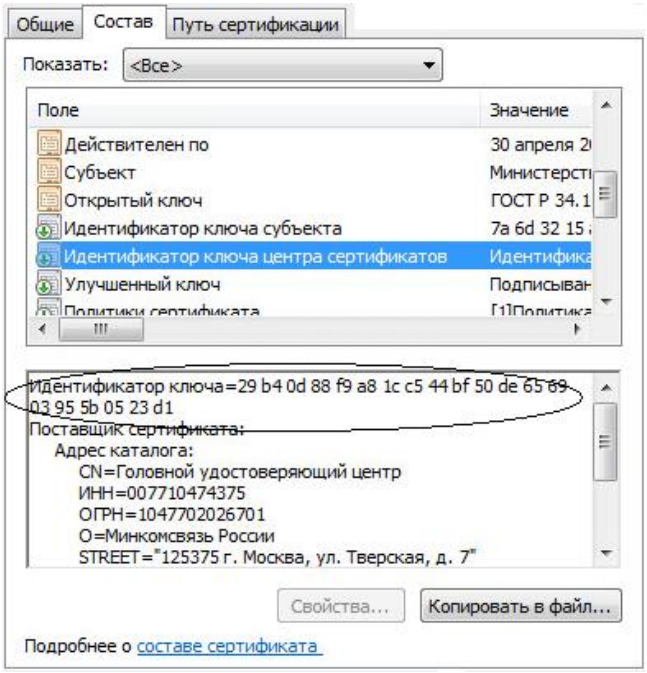


Рис. 25 Просмотр свойств сертификата автора подписи под TSL

3. Зайдите на портал уполномоченного федерального органа в области использования электронной подписи по адресу — https://e-trust.gosuslugi.ru/#/portal/mainca.
4. В перечне удостоверяющих центров найдите УЦ с соответствующим значением идентификатора ключа, как показано на Рис. 26.

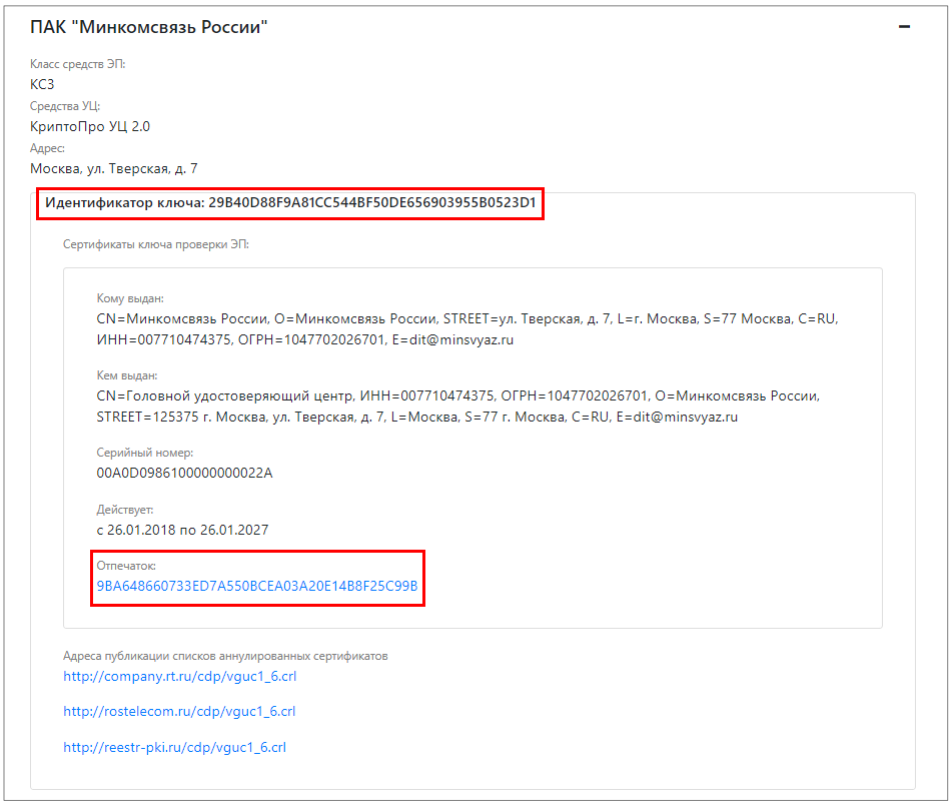


Рис. 26 Сведения о сертификате УЦ

5. Скачайте сертификат УЦ по ссылке на значении его отпечатка (хэш-кода), представленной на Рис. 26.
6. Зарегистрируйте сертификат УЦ на странице "Издатели" (см. стр. 16) **с указанием** адресов публикации CRL (см. стр. 18) и затем вторично, на странице "Управление TSL", **без указания** адресов публикации CRL.

Сертификат ГУЦ

Сертификат ГУЦ и адреса публикации CRL ГУЦ доступны на портале уполномоченного федерального органа в области использования электронной подписи по адресу — https://e-trust.gosuslugi.ru/#/portal/mainca.

Для регистрации сертификата ГУЦ:

1. Скачайте сертификат ГУЦ по ссылке на значении его отпечатка (хэш-кода), представленной на рисункеРис. 27.

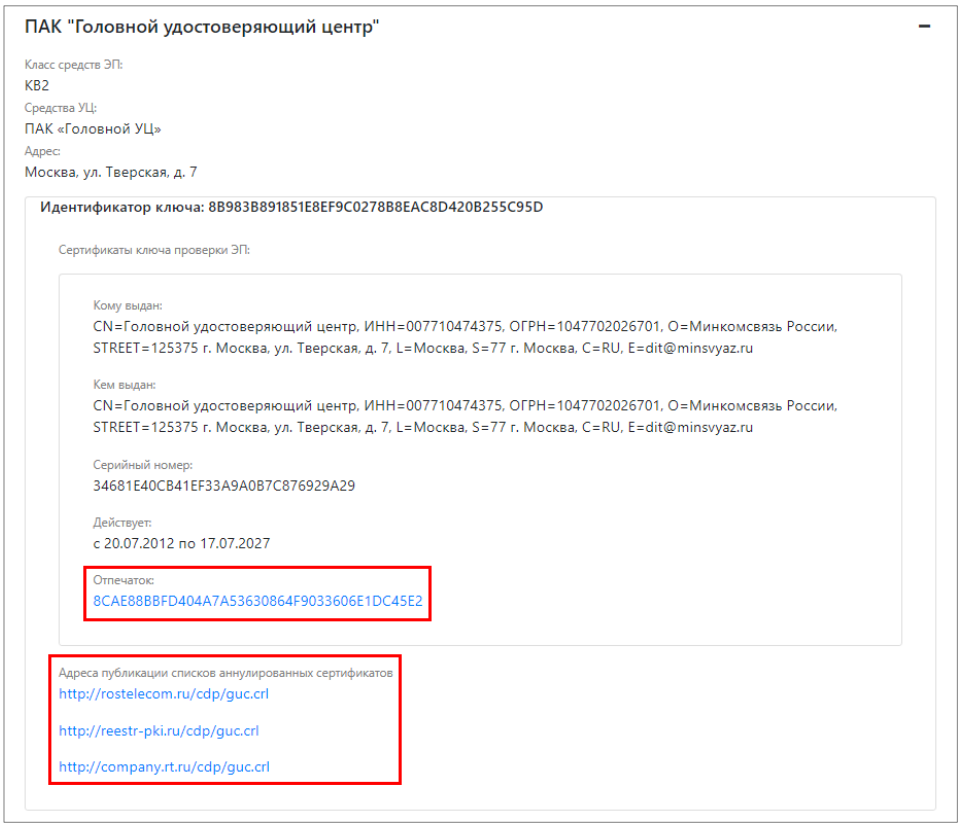


Рис. 27 Ссылка для скачивания сертификата ГУЦ и адреса публикации CRL ГУЦ

2. Зарегистрируйте сертификат ГУЦ на странице "Издатели" (см. стр. 16) **с указанием** адресов публикации CRL (см. стр. 18) и затем вторично, на странице "Управление TSL", **без указания** адресов публикации CRL.

Передача 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 Федеральный закон № 63 "Об электронной подписи" 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, выполнен в виде двух компонентов, один из которых (CAS–2) расположен во внешнем сегменте сети и решает задачи сбора списков, а второй (CAS–1) предоставляет собранные списки сервисам проверки подписи и разбора конфликтов. 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. Периодичность обмена зависит от общего регламента ИТ-системы и влияет только на степень актуальности списков отозванных сертификатов.

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 расширением ".crl".

Внимание! Запрещается использовать ключевые носители (отчуждаемые носители с записанными ключами ЭП, сертификатами) для передачи информации между компонентами CAS–1 и CAS–2.

Регламент обмена информацией между CAS–1 и CAS–2:

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. Извлечь носитель из USB-порта.
5. После этого необходимо снова подключить отчуждаемый носитель в компонент CAS–1 и отслеживать процесс использования носителя через консоль.
6. Извлечь носитель из USB-порта.

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.

Внимание! 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 файловой системы. Подобные действия приведут к некорректной работе системы.

Разбор конфликтных ситуаций с использованием АРМ РКС

Для доступа к сервису разбора конфликтов оператору необходимо в адресной строке штатного браузера ввести имя хоста или IP-адрес АРМ РКС с указанием порта подключения — 8083:

```
http://имя_хоста_или_IP-адрес_АРМ_РКС:8083
```

Графический интерфейс сервиса разбора конфликтов состоит из панели навигации с гиперссылками на страницы "Проверка ЭП" (загружается по умолчанию), "Процессы", "Общие настройки", "XSLT шаблон" и "Отчеты".

Проверка ЭП

На Рис. 28 представлен вид страницы "Проверка ЭП", предназначенной для проверки подписанного документа или отсоединенной ЭП на указанный момент времени.

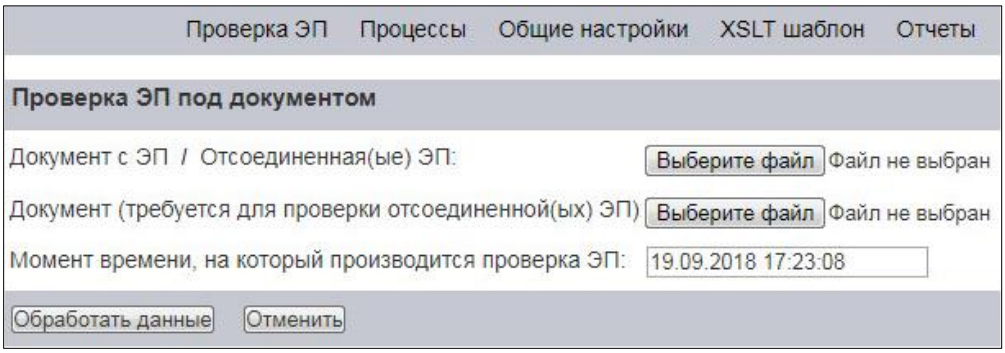


Рис. 28 Страница "Проверка ЭП"

Для проверки ЭП:

1. Нажмите кнопку "Выберите файл".

   На экране появится стандартный диалог выбора файла.

2. Выберите подписанный документ или отсоединенную ЭП, которые необходимо проверить (для отсоединенной ЭП дополнительно выбрать соответствующий документ).

3. Укажите дату (время) проверки и нажмите кнопку "Обработать данные".

   Если выбранный файл с ЭП имеет корректный формат данных, появится форма, содержащая информацию об имени издателя и серийном номере сертификата автора подписи, а также блок, предназначенный для добавления дополнительных данных в случае необходимости, как показано на Рис. 29.

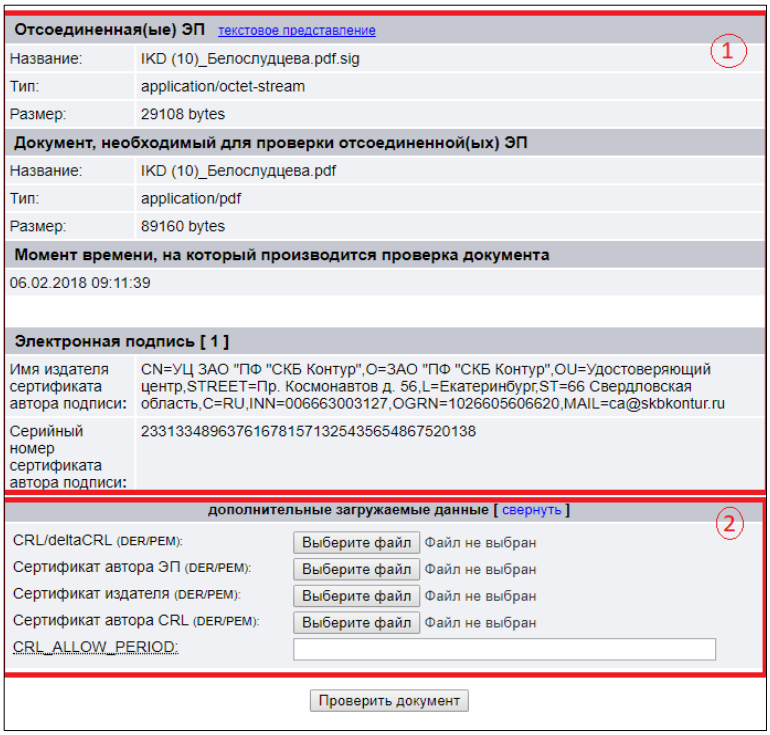


Рис. 29 Форма дополнительной информации об ЭП

4. Нажмите кнопку "Проверить документ".

   На экране появятся результаты проверки ЭП, как показано на Рис. 30.

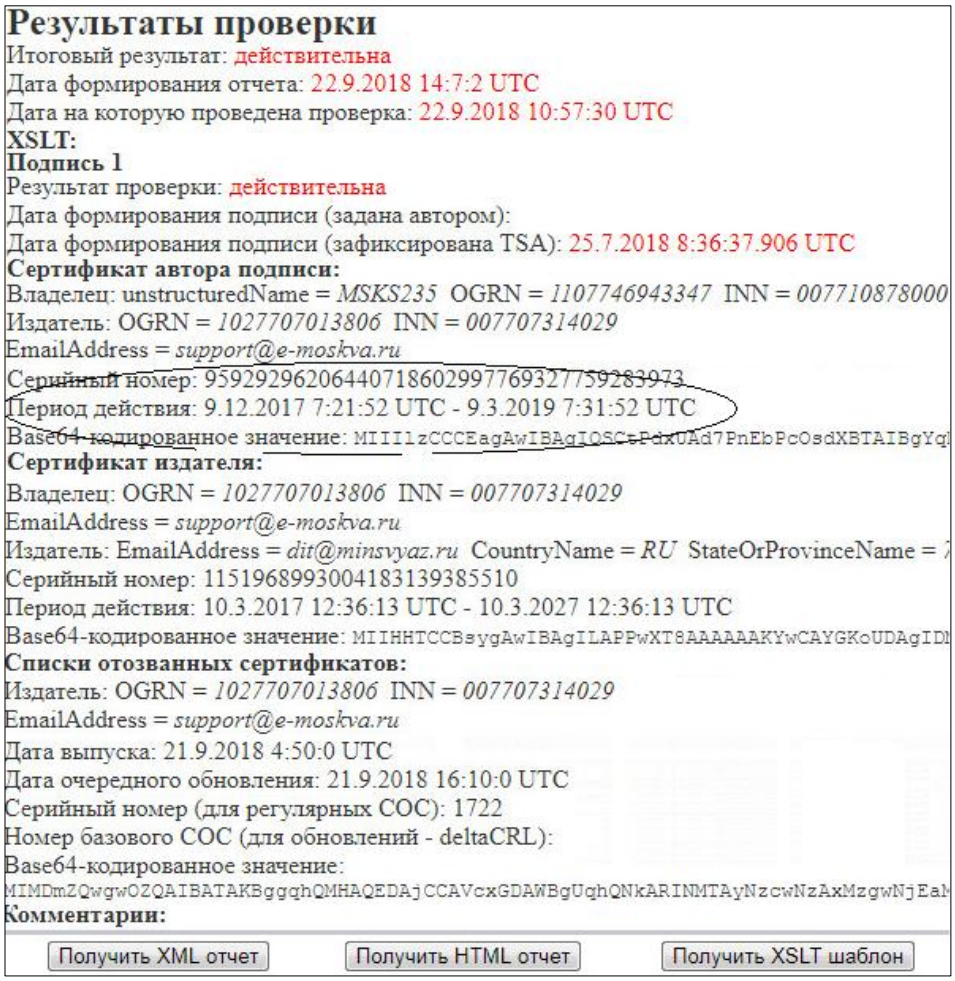
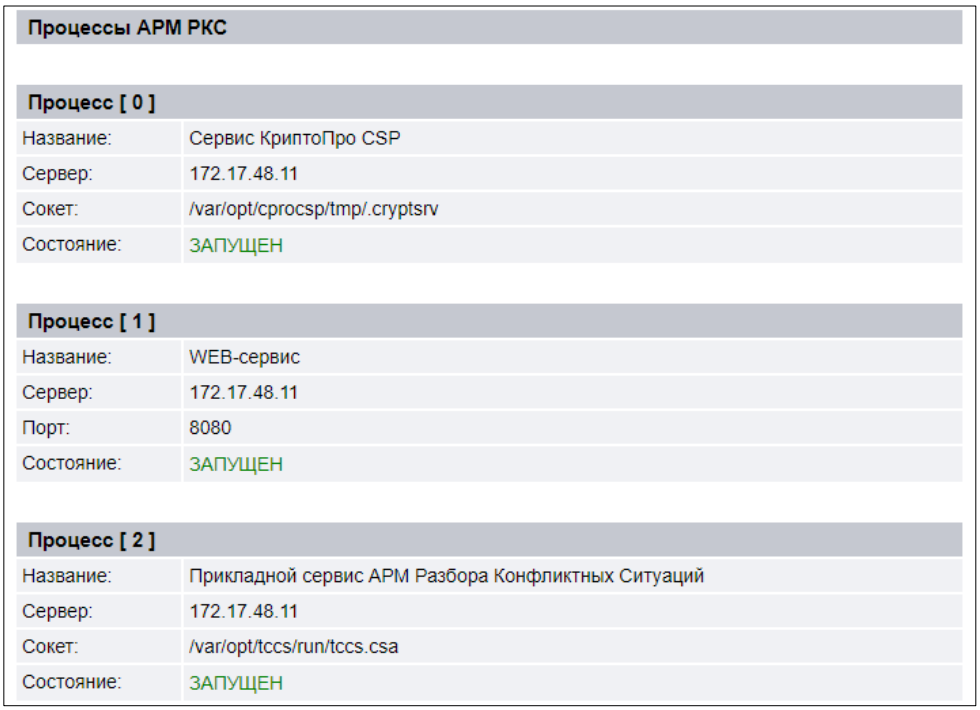


Рис. 30 Результаты проверки ЭП

Для формирования отчета о результатах проверки ЭП нажмите соответствующую кнопку — "Получить XML отчет", "Получить HTML отчет" и "Получить XSLT шаблон".

Мониторинг процессов АРМ РКС

На Рис. 31 представлен вид страницы "Процессы", показывающей основные показатели мониторинга процессов АРМ РКС — название, сервер, сокет и состояние. Оператору следует контролировать показатель процесса "Состояние" в режиме "ЗАПУЩЕН", а при переходе процесса в состояние "ОСТАНОВЛЕН" привлекать иных специалистов с ролями "системный программист (администратор)" и/или "программист" для устранения нештатной ситуации и запуска остановленного процесса.



Процессы АРМ РКС

Процесс [0]	
Название:	Сервис КриптоПро CSP
Сервер:	172.17.48.11
Сокет:	/var/opt/cprocsp/tmp/.cryptsrv
Состояние:	ЗАПУЩЕН

Процесс [1]	
Название:	WEB-сервис
Сервер:	172.17.48.11
Порт:	8080
Состояние:	ЗАПУЩЕН

Процесс [2]	
Название:	Прикладной сервис АРМ Разбора Конфликтных Ситуаций
Сервер:	172.17.48.11
Сокет:	/var/opt/tccs/run/tccs.csa
Состояние:	ЗАПУЩЕН

Рис. 31 Страница "Процессы"

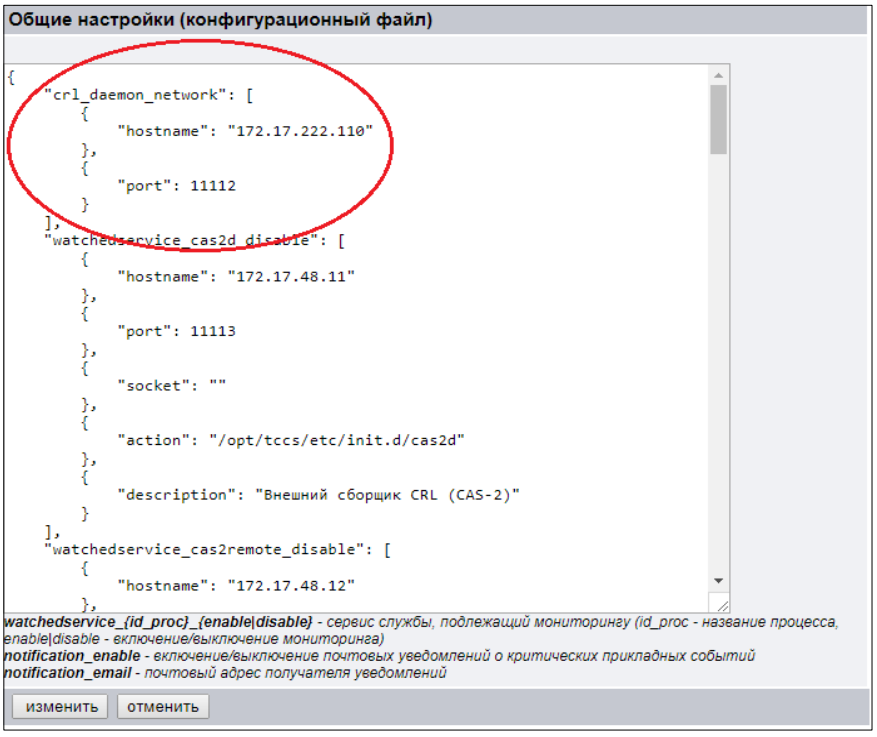
Настройка конфигурации АРМ РКС

На Рис. 32 представлен вид страницы "Общие настройки", предназначенной для оперативного изменения конфигурационного файла csm.conf АРМ РКС.

Настройку конфигурационного файла должны производить специалисты с ролями "системный программист (администратор)" и/или "программист".

Описание параметров конфигурационного файла csm.conf приведено в [**1**].

Оператору необходимо контролировать, что в поле crl_daemon_network указано имя хоста или IP-адрес того сервера CAS–1, от которого АРМ РКС получает данные о сертификатах УЦ и CRL в процессе разбора конфликтов при проверках ЭП.



Общие настройки (конфигурационный файл)

```
{
    "crl_daemon_network": [
        {
            "hostname": "172.17.222.110"
        },
        {
            "port": 11112
        }
    ],
    "watchedservice_cas2d_disable": [
        {
            "hostname": "172.17.48.11"
        },
        {
            "port": 11113
        },
        {
            "socket": ""
        },
        {
            "action": "/opt/tccs/etc/init.d/cas2d"
        },
        {
            "description": "Внешний сборщик CRL (CAS-2)"
        }
    ],
    "watchedservice_cas2remote_disable": [
        {
            "hostname": "172.17.48.12"
        },
```

watchedservice_{id_proc}_{enable|disable} *- сервис службы, подлежащий мониторингу (id_proc - название процесса, enable|disable - включение/выключение мониторинга)*
notification_enable *- включение/выключение почтовых уведомлений о критических прикладных событий*
notification_email *- почтовый адрес получателя уведомлений*

изменить | отменить

Рис. 32 Страница "Общие настройки"

XSLT-шаблон

На Рис. 33 представлен вид страницы "XSLT шаблон", предназначенной для задания шаблона формирования отчетов о результатах проверки ЭП.

Оператор имеет возможность получить и загрузить XSLT-шаблон формирования отчетов нажатием на соответствующие кнопки.

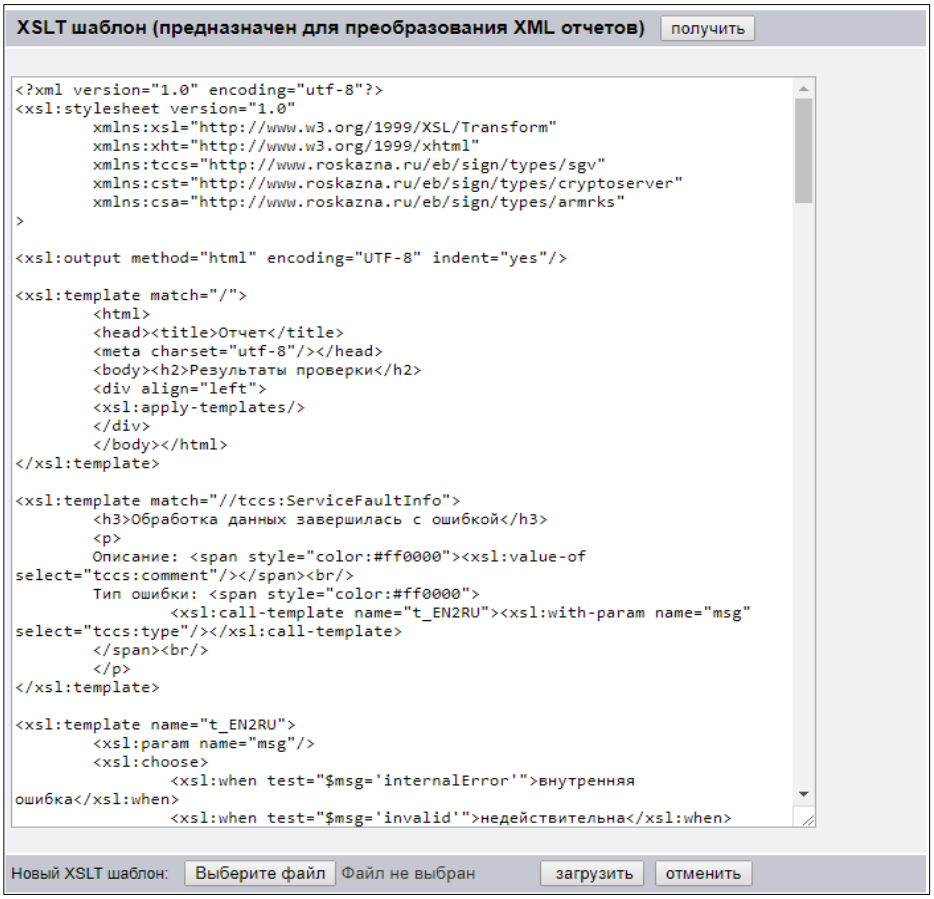


Рис. 33 Страница "XSLT шаблон"

Отчеты АРМ РКС

На Рис. 34 представлен вид страницы "Отчеты", предназначенной для формирования списка отчетов АРМ РКС о результатах проверки ЭП за указанный период.

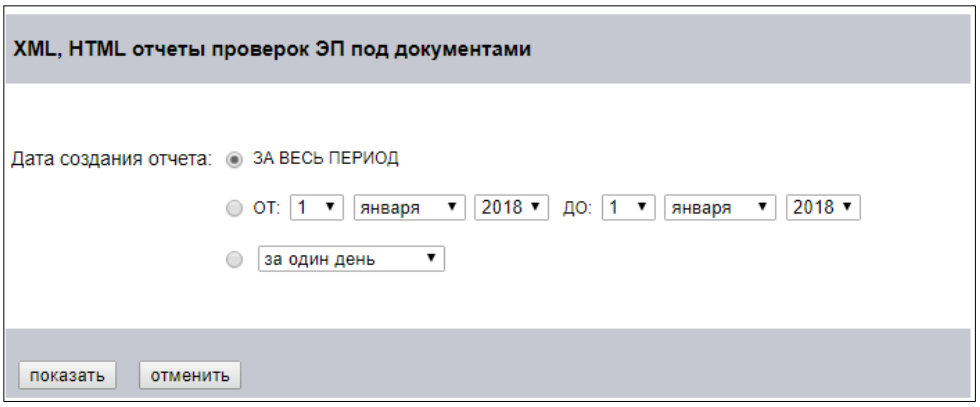


Рис. 34 Страница "Отчеты"

Для формирования списка отчетов:

1. Укажите временной интервал с помощью переключателя и значений из выпадающего списка.
2. Нажмите кнопку "показать".

На экране отобразится список отчетов (см. Рис. 35).

Список отчетов, содержащих результаты проверки ЭП под документом

1	06.02.2018 13:05	signature_txt	открыть	удалить
2	06.02.2018 12:55	IKD__10__Белослудцева_pdf_sig	открыть	удалить
3	06.02.2018 12:54	IKD__10__Белослудцева_pdf_sig	открыть	удалить
4	06.02.2018 12:33	IKD__10__Белослудцева_pdf_sig	открыть	удалить

Рис. 35 Список отчетов, содержащих результаты проверки ЭП

Список представляет полный перечень проверок ЭП, осуществлявшихся в АРМ РКС за указанный период времени, и позволяет просмотреть или удалить отчеты по ссылкам "открыть" и "удалить" соответственно.

Глава 4
Сообщения ПАК Jinn-Server

Компоненты ПАК Jinn-Server содержат в своем составе специальные модули, обеспечивающие мониторинг процессов (сервисов) и автоматический перезапуск в случае прерывания их работы. Оповещение обслуживающего персонала осуществляется по электронной почте на указанные в конфигурации адреса по факту следующих событий:

- процесс не запущен (прерван);
- произведена попытка запустить процесс автоматически;
- результат процедуры автоматического перезапуска.

Настройка конфигурации мониторинга процессов выполняется обслуживающим персоналом с ролью "программист" и описана в документе [**2**].

Документация

1. Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3. Руководство администратора.
2. Программно-аппаратный комплекс квалифицированной электронной подписи Jinn-Server. Версия 1.3. Руководство программиста.