Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

Руководство администратора безопасности

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 02
Версия	2.3
Листов	43
Дата	01.09.2025

Авторские права, товарные знаки, ограничения

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р.Д.»» без предварительного уведомления.

АО «Аладдин Р.Д.»» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р.Д.»» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р.Д.»» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р.Д.»» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.»» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую–либо страну, а также использоваться каким–либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в АО «Аладдин Р.Д.»», удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и АО «Аладдин Р.Д.»» (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного

Соглашения:

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

– не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

– не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

– не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

– не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому–либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (http://developer.aladdin–rd.ru/).

Использование ПО

Пользователь вправе:

– воспроизводить ПО путём записи его в память электронно–вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

– встраивать ПО любым способом в продукты и решения Пользователя;

– распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

– дизайна (графики, расположения элементов оформления и т.п.);

– всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких–либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантии

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие–либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

– заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

– возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого–либо использования данного программного обеспечения и/или любой компоненты данного по, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких–либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.»» за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

– лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

– вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую–либо страну, а также использоваться каким–либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого–либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

АННОТАЦИЯ

Данный документ содержит требования по безопасной эксплуатации программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»[1] при его эксплуатации совместно с СКЗИ «КрпитоПро CSP», его состав, назначение, компоненты, требования и условия эксплуатации.

Документ предназначен для Администраторов (Администраторов Безопасности), осуществляющих установку, обслуживание и контроль за соблюдением требований по безопасной эксплуатации программного средства, администраторов серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющих настройку рабочих мест для работы с программным средством, а также для пользователей программного средства.

[1] Далее по документу – программное средство

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММНОГО СРЕДСТВА

1.1 Область применения программного средства

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020 применяется как элемент систем защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации при идентификации и строгой аутентификации субъектов[1] и объектов доступа[2] в автоматизированной (информационной) системе.

Программное средство применяется при обработке информации, не содержащей сведения, составляющие государственную тайну, и может использоваться при реализации требований по защите информации от несанкционированного доступа для автоматизированных систем классов защищённости 1Д, 1Г.

Программное средство может применяться:

– при реализации мер защиты в государственных информационных системах до 1-го класса защищённости включительно;

– при обеспечении до 1-го уровня защищённости персональных данных, включительно, при их обработке в информационных системах персональных данных;

– при реализации мер защиты в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1-го класса защищённости включительно;

– в значимых объектах критической информационной инфраструктуры до 1-ой категории включительно;

– в информационных системах общего пользования II класса.

1.2 Состав программного средства Запуск и завершение программы

Программное средство включает:

1) Программный комплекс «Центр сертификации Aladdin Enterprise Certification Authority»[3] RU.АЛДЕ.03.01.038, состоящий из следующих программных компонентов:

– Программный компонент «Серверная часть Центра сертификации»[4] RU.АЛДЕ.03.01.040. Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов безопасности цифровых сертификатов) (далее – сертификаты), выпуска и обслуживания сертификатов, приостановки и/или возобновления действия сертификатов, предоставления информации о сертификатах и их статусах.

[1] Субъектами доступа могут являться как физические лица (пользователи), так и ресурсы автоматизированной информационной системы, а также вычислительные процессы, инициирующие получение и получающие доступ от имени пользователей, программ, средств вычислительной техники и других программно-аппаратных устройств информационно-телекоммуникационной инфраструктуры.

[2] Объект доступа представляет собой одну из сторон информационного взаимодействия, предоставляющую доступ.

[3] Далее по документу – Центр сертификации.

[4] Далее по документу – Серверная часть Центра сертификации.

– Программный компонент «Клиентская часть Центра сертификации»[1] RU.АЛДЕ.03.01.041. Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра сертификации» RU.АЛДЕ.03.01.040.

2) Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority»[2] RU.АЛДЕ.03.01.039, состоящий из следующих программных компонентов:

– Программный компонент «Серверная часть Центра валидации»[3] RU.АЛДЕ.03.01.042. Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части предоставления информации о сертификатах и их статусах.

– Программный компонент «Клиентская часть Центра валидации»[4] RU.АЛДЕ.03.01.043. Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра валидации» RU.АЛДЕ.03.01.042.

3) Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority»[5] RU.АЛДЕ.03.01.051, состоящий из следующих программных компонентов:

– Программный компонент «Серверная часть Центра регистрации»[6] RU.АЛДЕ.03.01.052. Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов, выпуска и обслуживания сертификатов.

– Программный компонент «Клиентская часть Центра регистрации»[7] RU.АЛДЕ.03.01.053. Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации» RU.АЛДЕ.03.01.052.

4) Программное средство «Утилита контроля целостности 2.0» RU.АЛДЕ.02.13.002-09. Программное средство предназначена для контроля целостности исполняемых файлов и дистрибутивов программных комплексов из состава Центра сертификатов доступа.

5) Средство криптографической защиты информации «КриптоПро CSP» версии 5.0 R3 КС1 (исполнение 1-Base) ЖТЯИ.00101-03 или версии 5.0 R3 КС2 (исполнение 2-Base) ЖТЯИ.00102-03 [8]. Средство криптографической защиты информации (далее – СКЗИ) предназначено для создания, хранения и удаления ключевых пар (открытый и

[1] Далее по документу – Клиентская часть Центра сертификации.
[2] Далее по документу – Центр валидации.
[3] Далее по документу – Серверная часть Центра валидации.
[4] Далее по документу – Клиентская часть Центра валидации.
[5] Далее по документу – Центр регистрации.
[6] Далее по документу – Серверная часть Центра регистрации.
[7] Далее по документу – Клиентская часть Центра регистрации.
[8] СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки программного средства и, при необходимости, приобретается заказчиком самостоятельно. Порядок настройки взаимодействия Центра сертификации с СКЗИ «КриптоПро CSP» описан в Приложении 5. Порядок настройки взаимодействия Центра регистрации Aladdin eRA с СКЗИ «КриптоПро CSP» описан в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 5. Центр регистрации Aladdin Enterprise Registration Authority». Порядок настройки взаимодействия Центра валидации Aladdin eVA с СКЗИ «КриптоПро CSP» описан в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority».

закрытый ключи) центров сертификации инфраструктуры открытых ключей, создания ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств), генерации и проверки цифровой подписи, а также для идентификации, аутентификации, шифрования и имитозащиты TLS-соединений.

6) Программно-аппаратный криптографический модуль «КриптоПро HSM» версии 2.0 R3 ЖТЯИ.00096-01 (исполнение 1К, комплектация 1 или 2)[1]. Программно-аппаратный криптографический модуль (далее – ПАКМ) предназначен для создания, хранения и удаления ключевых пар (открытый и закрытый ключи) центров сертификации инфраструктуры открытых ключей, создания ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств), а также генерации и проверки цифровой подписи.

1.3 Основные функции программного средства

Программное средство реализует следующие функции:

1) Формирование идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств) (далее по тексту – СВТ) на основе данных, полученных при первичной идентификации непосредственно от пользователей и СВТ через заявку на выпуск сертификатов, либо полученных от доменной службы каталогов или уполномоченных пользователей. Первичная идентификация пользователей и СВТ в программном средстве завершается созданием для них субъектов. Идентификационная информация, необходимая для выпуска сертификатов, представляет собой атрибуты субъекта, значения которых записываются в поля сертификатов, создаваемых для данного субъекта.

2) Выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:

– Создание ключевых пар (открытый и закрытый ключи) пользователей и СВТ. Создание ключевых пар для пользователей и средств вычислительной техники (устройств) выполняется при формировании для них сертификатов с закрытым ключом (PKCS#12) [2].

– Формирование сертификатов для пользователей и СВТ. В программном средстве реализовано формирование сертификатов для пользователей и СВТ:

  – С закрытым ключом (PKCS#12).
  – На основании запроса PKCS#10 [3].

– Формирование заявок на выпуск сертификатов для пользователей и СВТ. В программном средстве реализовано:

  – Создание заявок пользователями с ролями «Администратор» и «Оператор» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации».

[1] ПАКМ «КриптоПро HSM» не является обязательным программным средством, не входит в комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно.

[2] В соответствии с документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1».

[3] В соответствии с документом «RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7».

- Создание заявок пользователем с ролью «Получатель сертификата» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации», включая заявки, создаваемые через программный интерфейс по протоколу WS-Trust X.509v3 Token Enrollment Extensions (WSTEP) [1].
- Создание заявок через программный интерфейс программного компонента «Серверная часть Центра регистрации» по протоколу Simple Certificate Enrollment Protocol (SCEP) [2].
- Автоматическое создание заявок на основании запросов PKCS#10 из локального или сетевого каталога в соответствии с настройками Offline-выпуска.

– Выдача сертификатов для их использования владельцами. Выдача сертификатов для их использования владельцами доступна:

- Путем их экспорта за пределы программного средства пользователями с ролями «Администратор» или «Оператор».
- Путем их экспорта за пределы программного средства инициатором заявки на выпуск сертификата, если по данной заявке успешно выпущен сертификат.
- Путем их автоматического экспорта за пределы программного средства в локальный или сетевой каталог в соответствии с настройками Offline-выпуска.

– Централизованное автоматическое (автоматизированное) отслеживание актуальности (с уведомлением владельцев о сроках действия) сертификатов. Уведомление владельцев о сроках действия их сертификатов выполняется по электронной почте. По умолчанию программное средство уведомляет владельца сертификата в случае, если срок его действия истекает через 30 суток, через 7 суток или через 1 сутки. В программном средстве доступно формирование шаблонов рассылок уведомлений владельцев о сроках действия их сертификатов. Для каждого шаблона рассылки доступно указание времени, отслеживаемого до окончания действия сертификата, а также текста отправляемого уведомления.

3) Выпуск и обслуживание сертификатов центров сертификации инфраструктуры открытых ключей, в том числе:

– Создание, экспорт, импорт и удаление ключевой пары (открытый и закрытый ключи) центра сертификации (корневого и/или подчиненного). Создание ключевой пары центра сертификации (корневого и/или подчиненного) выполняется при создании собственного центра сертификации в программном средстве. В программном средстве доступно создание центра сертификации (корневого и/или подчиненного) на основании импортированного контейнера закрытого ключа PKCS #12 центра сертификации, содержащего его ключевую пару. Для центра сертификации доступен экспорт ключевой пары за пределы программного средства, если его ключевая пара уже не экспортирована за пределы программного средства, и для данной ключевой пары при ее создании не был установлен запрет на экспорт. При экспорте ключевая пара центра сертификации удаляется из программного средства. Для центра сертификации, ключевая пара которого экспортирована за пределы программного средства, доступна возможность импорта его ключевой пары в программное средство. Удаление ключевой пары центра

[1] В соответствии с документом «OASIS WS-Trust 1.3. WS-Trust X.509 Token Profile (WSTEP)».

[2] В соответствии с документом «RFC 8894. Simple Certificate Enrolment Protocol».

сертификации выполняется при удалении данного центра сертификации из программного средства, если его ключевая пара уже не экспортирована за пределы программного средства.

– Создание, импорт, просмотр, экспорт и удаление корневого (самоподписанного) сертификата центра сертификации.

– Создание, просмотр, экспорт и удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации.

– Создание на основании запроса, импорт, просмотр, экспорт, удаление и отзыв сертификата для подчиненного центра сертификации. Создание сертификата для подчиненного центра сертификации на основании запроса выполняется в вышестоящем центре сертификации при подписании запроса на сертификат данного подчиненного центра сертификации. Импорт сертификата для подчиненного центра сертификации выполняется при создании в программном средстве подчиненного центра сертификации на основании импортированного контейнера закрытого ключа PKCS #12 подчиненного центра сертификации. В программном средстве доступен просмотр значений полей созданного сертификата для подчиненного центра сертификации. Сертификат для подчиненного центра сертификации доступен для экспорта за пределы программного средства как отдельно, так и в составе его цепочки сертификатов. Удаление сертификата подчиненного центра сертификации выполняется при удалении данного центра сертификации из программного средства. В вышестоящем центре сертификации, подписавшем запрос на сертификат подчиненного центра сертификации, доступен отзыв сертификата данного подчиненного центра сертификации.

4) Приостановка и/или возобновление действия пользователей и СВТ, в том числе:

– Блокирование, возобновление действия, отзыв и перевыпуск сертификатов.

– Формирование, экспорт и публикация списка отозванных сертификатов. Формирование списка отозванных сертификатов выполняется автоматически с задаваемой пользователем с ролью «Администратор» периодичностью и/или при любом изменении статуса сертификата. В программном средстве доступен экспорт списка отозванных сертификатов. При каждом формировании списка отозванных сертификатов безопасности выполняется его публикация в зарегистрированные точки распространения. В программном средстве доступна публикация списка отозванных сертификатов и сертификатов центров сертификации в точки распространения центров валидации, создаваемых в Центре валидации, и точки распространения доменной службы каталогов.

5) Предоставление информации о сертификатах центров сертификации, пользователей и СВТ, а также информации об их статусах, в том числе:

– Формирование и экспорт реестра сертификатов. В программном средстве реализовано формирование реестра сертификатов, содержащего значения полей всех созданных сертификатов. При экспорте реестра сертификатов доступен выбор критериев, которым должны соответствовать сертификаты в экспортируемом реестре.

– Проверка статусов сертификатов на основании данных, опубликованных в точке распространения. Программное средство позволяет экспортировать опубликованные списки отозванных сертификатов и сертификаты центров сертификации из точек распространения, реализованных программным средством.

– Проверка статусов сертификатов в режиме реального времени. Программное средство позволяет выполнять проверку статусов сертификатов в режиме реального времени по протоколу Online Certificate Status Protocol (OCSP) [1].

Центр сертификатов доступа выпускает сертификаты в следующих форматах:

1) Формат сертификата открытого ключа X.509v3 [2]. Сертификат включает в себя следующие данные:

– Версия сертификата.
– Серийный номер сертификата.
– Идентификатор алгоритма подписи сертификата.
– Отличительное имя издателя сертификата.
– Период действия сертификата.
– Отличительное имя субъекта.
– Информация об открытом ключе, включающая алгоритм открытого ключа и сам открытый ключ.
– Расширения сертификата, включая следующие возможные поля:
  – Идентификатор ключа издателя сертификата.
  – Идентификатор ключа субъекта.
  – Идентификаторы использования ключа.
  – Политики сертификата.
  – Альтернативное имя субъекта.
  – Альтернативное имя издателя сертификата.
  – Базовые ограничения.
  – Точки распространения списков отзыва.
  – Доступ к информации о центрах сертификации.
  – Идентификаторы расширенного использования ключа.
– Подпись сертификата.

2) Формат списка отозванных сертификатов безопасности (CRL) [3]. Список отозванных сертификатов включает в себя следующие данные:

– Версия CRL.
– Отличительное имя издателя CRL.
– Дата и время издания текущего CRL.
– Дата и время издания следующего CRL.
– Расширения CRL, включая следующие возможные поля:
  – Идентификатор ключа издателя CRL.
  – Номер CRL.

[1] В соответствии с документом «RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP».

[2] Формат определяется документом «ITU-T Recommendation X.509 (10/2019). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks».

[3] Формат определяется документом «ITU-T Recommendation X.509 (10/2019). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks».

- Перечень отозванных сертификатов, где для каждого сертификата указаны:
  - Серийный номер.
  - Дата и время отзыва.
  - Причина отзыва (может отсутствовать).
- Алгоритм подписи CRL.
- Подпись CRL.

3) Формат контейнера закрытого ключа PKCS #12 [1]. Контейнеры закрытого ключа включают в себя следующие данные:

- Цепочка сертификатов владельца закрытого ключа.
- Закрытый ключ.

Центр сертификатов доступа реализовывает следующие криптографические алгоритмы:

4) Алгоритмы генерации ключевой пары:

- RSA с длинами ключей 1024, 1536, 2048, 3072, 4096, 6144 и 8192 бит.
- ECDSA с длинами ключей 256, 384 и 521 бит.
- ГОСТ Р 34.10-2012 с ключом 256 или 512 бит [2].

5) Алгоритмы генерации цифровой подписи:

- RSA PKCS#1 Ver 1.5 (длины ключей: 1024, 1536, 2048, 3072, 4096, 6144 и 8192 бит; хэш-алгоритмы: SHA256, SHA384, SHA512).
- ECDSA (длины ключей: 256, 384, 521 бит; хэш-алгоритмы: SHA256, SHA384, SHA512).
- ГОСТ Р 34.10-2012 с ключом 256 или 512 бит (хэш-алгоритм: ГОСТ Р 34.11-2012 с длиной хэш-кода 256 или 512 бит) [3].

[1] Формат определяется документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1»

[2] Данный алгоритм доступен при использовании СКЗИ «КриптоПро CSP» в составе Центра сертификации Aladdin eCA.

[3] Данный алгоритм доступен при использовании СКЗИ «КриптоПро CSP» в составе Центра сертификации Aladdin eCA.

1.4 Условия эксплуатации программного средства

1.4.1 Условия эксплуатации Центра сертификации

В данном разделе приведены аппаратно-программные требования, предъявляемые к СФ Центра сертификации. СФ серверной и клиентской частей Центра сертификации являются СВТ, представляющие совокупность аппаратных средств (далее – АС) и программного обеспечения (далее – ПО), требования к составу которых представлены в таблицах 1 и 2 соответственно.

Таблица 1 - АС и ПО, необходимые для функционирования серверной части Центра сертификации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	12, не менее
Машинный носитель информации с объемом свободного места, Гбайт	50, не менее
Программное обеспечение	
Сертифицированная операционная система (далее – ОС) семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Сертифицированная система управления базами данных (далее – СУБД)	– PostgreSQL из состава ОС – Postgres Pro – Jatoba
Веб-сервер	Cpnginx из состава средства СКЗИ «КриптоПро CSP» версии 5.0 R3
Среда разработки и исполнения	Java Axiom JDK Certified
Сертифицированное СКЗИ (опционально)	– СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) – СКЗИ «КриптоПро CSP» версия 5.0 R3 КС2 (исполнение 2-Base)

Таблица 2 – АС и ПО, необходимые для функционирования клиентской части Центра сертификации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	4, не менее
Машинный носитель информации с объемом свободного места, Гбайт	50, не менее
Программное обеспечение	
Сертифицированная ОС семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Браузер	Из состава ОС

1.4.2 Условия эксплуатации Центра регистрации

В данном разделе приведены аппаратно-программные требования, предъявляемые к СФ Центра регистрации. СФ серверной и клиентской частей Центра регистрации являются СВТ, представляющие совокупность аппаратных средств (далее – АС) и программного обеспечения (далее – ПО), требования к составу которых представлены в таблицах 3 и 4 соответственно.

Таблица 3 - АС и ПО, необходимые для функционирования серверной части Центра регистрации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	8, не менее
Машинный носитель информации с объемом свободного места, Гбайт	50, не менее
Программное обеспечение	
Сертифицированная операционная система (далее – ОС) семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Сертифицированная система управления базами данных (далее – СУБД)	– PostgreSQL из состава ОС – Postgres Pro – Jatoba
Веб-сервер	Cpnginx из состава средства СКЗИ «КриптоПро CSP» версии 5.0 R3
Среда разработки и исполнения	Java Axiom JDK Certified
Сертифицированное СКЗИ (опционально)	– СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) – СКЗИ «КриптоПро CSP» версия 5.0 R3 КС2 (исполнение 2-Base)

Таблица 4 – АС и ПО, необходимые для функционирования клиентской части Центра регистрации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	4, не менее
Машинный носитель информации с объемом свободного места, Гбайт	50, не менее
Программное обеспечение	
Сертифицированная ОС семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Браузер	Из состава ОС

1.4.3 Условия эксплуатации Центра валидации

В данном разделе приведены аппаратно-программные требования, предъявляемые к СФ Центра валидации. СФ серверной и клиентской частей Центра валидации являются СВТ, представляющие совокупность аппаратных средств (далее – АС) и программного обеспечения (далее – ПО), требования к составу которых представлены в таблицах 5 и 6 соответственно.

Таблица 5 - АС и ПО, необходимые для функционирования серверной части Центра валидации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	4, не менее
Машинный носитель информации с объемом свободного места, Гбайт	20, не менее
Программное обеспечение	
Сертифицированная операционная система (далее – ОС) семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Сертифицированная система управления базами данных (далее – СУБД)	– PostgreSQL из состава ОС – Postgres Pro – Jatoba
Веб-сервер	Cpnginx из состава средства СКЗИ «КриптоПро CSP» версии 5.0 R3
Среда разработки и исполнения	Java Axiom JDK Certified
Сертифицированное СКЗИ (опционально)	– СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) – СКЗИ «КриптоПро CSP» версия 5.0 R3 КС2 (исполнение 2-Base)

Таблица 6 – АС и ПО, необходимые для функционирования клиентской части Центра валидации

Параметры технического (аппаратного) средства или программное обеспечение	Значения параметров технического (аппаратного) средства или программное обеспечение
Аппаратные средства	
Процессор архитектуры x86 или x64	Двухъядерный процессор с тактовой частотой 2400 MHz, не менее
Оперативное запоминающее устройство, Гбайт	4, не менее
Машинный носитель информации с объемом свободного места, Гбайт	20, не менее
Программное обеспечение	
Сертифицированная ОС семейства Linux	– Операционная система специального назначения «Astra Linux Special Edition» – Операционная система «РЕД ОС» – Операционная система Альт 8 СП – Операционная система Platform V SberLinux OS Server
Браузер	Из состава ОС

1.5 Перечень пользовательских интерфейсов программного средства

1.5.1 Интерфейс командной строки операционной системы

Командная строка ОС доступна для пользователя с ролью «Администратор» (далее – Администратор). Управление серверной частью выполняется с помощью запуска bash-скриптов, входящих в его состав.

1.5.2 Веб-интерфейс

В адресной строке браузера ввести IP-адрес или полное доменное имя веб-сервера соответствующего компонента. Веб-интерфейс становится доступен после успешной идентификации и аутентификации пользователя с помощью сертификата. Полномочия пользователя посредством веб-интерфейса зависят от его роли.

1.5.3 Программный интерфейс серверного приложения

В составе серверной части Центра сертификации реализован программный интерфейс REST API, который предоставляет пользователю следующие методы:

- метод аутентификации пользователя по сертификату доступа;
- метод идентификации и аутентификации пользователя по маркеру доступа;
- метод генерации и предоставления нового маркера доступа при истечении срока действия текущего маркера доступа;
- метод поиска сессии пользователя;
- метод завершения активных сессий пользователей;
- метод создания учетной записи пользователя;
- метод удаления сессии пользователя;
- метод получения списка учетных записей пользователей;
- метод получения учетной записи пользователя по идентификатору;
- метод изменения параметров учетной записи пользователя;
- метод удаления учетной записи пользователя;
- метод отвязки субъектов от учетных записей;
- метод блокирования активной учетной записи;
- метод активации заблокированной учетной записи;
- метод обновления активности учетной записи;
- метод создания правил доступа;
- метод редактирования правил доступа по идентификатору;
- метод удаления правила доступа;
- метод получения списка правил доступа;
- метод получения правила доступа по идентификатору;
- метод проверки наличия доступа у субъекта доступа к объектам доступа по существующим правилам доступа;
- метод проверки наличия доступа у субъекта доступа к модулю по существующим в программе правилам

доступа;

– метод проверки наличия доступа у субъекта доступа к ресурсу по существующим в программе правилам доступа;

– метод проверки существования правила доступа;

– метод распределения запросов пользователей между программными интерфейсами модулей;

– метод предоставления информации об установленной лицензии;

– метод проверки лицензии перед импортом;

– метод импорта (установки) лицензии.

– метод сохранения записи аудита в базу данных;

– метод получения записей аудита из базы данных;

– метод выставления метки об удалении учетной записи пользователя всем событиям в журнале;

– метод создания записи о новом syslog-сервере;

– метод редактирования записи о syslog-сервере;

– метод удаления записи о syslog-сервере;

– метод активации публикации сообщений с информацией о событиях аудита для syslog-сервера;

– метод выключения публикации сообщений с информацией о событиях аудита для syslog-сервера;

– метод получения списка созданных записей о syslog-серверах;

– метод получения данных Syslog-сервера по его идентификатору.

– метод создания сертификатов и контейнеров закрытого ключа для пользователей и субъектов;

– метод создания сертификатов для субъектов и подчиненных центров сертификации на основании запроса на сертификат;

– метод валидации запроса на сертификат на соответствие шаблону и атрибутам субъекта;

– метод перевыпуска сертификата доступа по запросу;

– метод создания центра сертификации на основе внешнего ключа;

– метод создания корневого центра сертификации, а также создания его сертификата и контейнера закрытого ключа;

– метод создания подчиненного центра сертификации, запроса на сертификат подчиненного центра сертификации, а также для создания его контейнера закрытого ключа;

– метод загрузки цепочки сертификатов для подчиненного центра сертификации;

– метод получения данных о выпущенных сертификатах;

– метод получения данных о сертификате с выбранным идентификатором;

– метод получения данных о сертификате с выбранным серийным номером;

– метод получения данных о сертификате с выбранным отпечатком сертификата;

– метод подсчета количества сертификатов в программе;

– метод получения данных о созданных центрах сертификации;

– метод получения данных о центре сертификации с выбранным идентификатором;

– метод получения данных об активном центре сертификации, включая данные его сертификата;

- метод подсчета количества центров сертификации;
- метод получения сертификата по идентификатору центра сертификации;
- метод активации центра сертификации;
- метод загрузки цепочки сертификатов для подчиненного центра сертификации;
- метод удаления центра сертификации;
- метод генерации списка отозванных сертификатов (CRL);
- метод расшифрования контейнера закрытого ключа;
- метод расшифрования сертификата;
- метод расшифрования контейнера сертификата;
- метод предназначен отзыва или приостановки действия сертификатов;
- метод активации приостановленных сертификатов;
- метод публикации сертификата в ресурсную систему;
- метод отражения статуса публикации сертификата в ресурсную систему;
- метод отзыва или приостановки действия выбранного сертификата;
- метод активации выбранного приостановленного сертификата;
- метод предоставления информации о доступных криптопровайдерах криптографических алгоритмов;
- метод импорта контейнера закрытого ключа центра сертификации;
- метод экспорта контейнера закрытого ключа центра сертификации;
- метод валидации контейнера закрытого ключа центра сертификации;
- метод получения информации о контейнере закрытого ключа центра сертификации;
- метод получения контейнера закрытого ключа центра сертификации;
- метод получения данных о существующих шаблонах сертификатов;
- метод просмотра данных шаблона с выбранным идентификатором;
- метод редактирования параметров шаблона с выбранным идентификатором;
- метод создания шаблона по запросу;
- метод копирования шаблона с выбранным идентификатором;
- метод удаления всех шаблонов;
- метод удаления с выбранным идентификатором;
- метод удаления шаблона по идентификатору центра сертификации;
- метод импорта шаблонов сертификатов из файлов;
- метод создания расширенного использования ключа;
- метод получения списка расширенных использований ключа;
- метод получения расширенного использования ключа по его идентификатору;
- метод получения расширенного использования ключа по OID;
- метод удаления расширенного использования ключа по идентификатору.
- метод установки контейнера закрытого ключа и сертификата веб-сервера ОС (СФ);
- метод предоставления данных текущего сертификата веб-сервера ОС (СФ);

- метод предоставления информации о программе;
- метод запуска процесса инициализации программы;
- метод создания издателя сертификатов доступа;
- метод активации издателя сертификатов доступа по идентификатору центра сертификации;
- метод отключения издателя сертификатов доступа по идентификатору центра сертификации;
- метод предоставления списка разрешенных издателей сертификатов;
- метод предоставления данных издателя сертификатов по идентификатору центра сертификации;
- метод удаления издателя сертификатов из списка разрешенных издателей по идентификатору центра сертификации;
- метод предоставления списка доступных пользователю страниц веб-интерфейса в соответствии с его ролью.
- метод предоставления списка субъектов ресурсных систем;
- метод предоставления данных субъекта ресурсной системы по его идентификатору;
- метод предоставления списка идентификаторов субъектов;
- метод предоставления количества субъектов;
- метод обновления (создания) субъекта;
- метод обновления (создания) субъекта на основании запроса pkcs#10;
- метод удаления субъекта по его идентификатору;
- метод получения данных созданных точек подключения к ресурсным системам;
- метод создания новой точки подключения к ресурсной системе;
- метод редактирования параметров существующей точки подключения к ресурсным системам;
- метод удаления точки подключения к ресурсной системе по ее идентификатору;
- метод синхронизации данных точки подключения к ресурсной системе по ее идентификатору;
- метод получения параметров точки подключения к ресурсной системе по ее идентификатору;
- метод синхронизации данных ресурсной системы;
- метод получения данных по всем доступным ресурсным системам;
- метод получения данных ресурсной системы по ее идентификатору;
- метод удаления ресурсной системы;
- метод публикации сертификата в ресурсную систему;
- метод получения данных о опубликованных сертификатах;
- метод получения данных о опубликованных сертификатах по идентификатору сертификата;
- метод очистки опубликованных сертификатов.
- метод получения файлов из хранилища;
- метод сохранения файлов в хранилище;
- метод удаления файлов из хранилища;
- метод получения файла из хранилища с выбранным идентификатором.
- метод экспорта файла запроса на сертификат;

- метод экспорта файла контейнера закрытого ключа;
- метод экспорта файла Delta CRL;
- метод экспорта файла списка отозванных сертификатов (CRL);
- метод экспорта файла цепочки сертификатов;
- метод экспорта файла цепочки сертификатов центра сертификации;
- метод экспорта файла сертификата;
- метод экспорта файла сертификата центра сертификации;
- метод экспорта файла корневого сертификата центра сертификации;
- метод создания задачи по формированию файла с записями журнала событий;
- метод создания задачи по формированию файла с данными выпущенных сертификатов;
- метод повторного запуска задачи по формированию файла, содержащего в себе записи аудита или данные сертификатов;
- метод экспорта файла с записями журнала событий или данными выпущенных сертификатов;
- метод получения информации о задачах по формированию файлов с записями о событиях аудита или данными сертификатов.
- метод получения электронной почты субъекта для оправки уведомлений об истечении срока действия его сертификата;
- метод создания сертификатов для получения списка сертификатов, соответствующих шаблонам рассылки уведомлений;
- метод создания нового шаблона рассылки;
- метод получения шаблона рассылки по идентификатору;
- метод получения шаблона по типу рассылки;
- метод редактирования (обновления) шаблона рассылки по идентификатору;
- метод активации шаблона рассылки по идентификатору;
- метод отключения шаблона рассылки по идентификатору;
- метод удаления шаблона рассылки по идентификатору.
- метод создания нового центра валидации;
- метод создания службы OCSP;
- метод подключения службы OCSP по идентификатору;
- метод получения опубликованного сертификата текущего издающего центра сертификации (AIA) из точки распространения CRL для центра валидации;
- метод получения расширенной информации о центре валидации по его идентификатору;
- метод удаления по идентификатору центра валидации;
- метод удаления центров валидации;
- метод получения информации о доступных в программе службах OCSP;
- метод получения информации по идентификатору о службе OCSP;
- метод получения опубликованного сертификата текущего издающего центра сертификации (AIA) из

точки распространения CRL для центра валидации;

- метод получения расширенной информации о центре валидации по его идентификатору;
- метод удаления по идентификатору центра валидации;
- метод удаления центров валидации;
- метод получения информации о доступных в программе службах OCSP;
- метод получения информации по идентификатору о службе OCSP;
- метод обновления информации по идентификатору о службе OCSP;
- метод приоритезации службы OCSP;
- метод кластеризации службы OCSP;
- метод активации службы OCSP;
- метод деактивации службы OCSP;
- метод удаления по идентификатору службы OCSP;
- метод удаления всех служб OCSP;
- метод получения информации по идентификатору о центре валидации;
- метод получения информации о доступных в программе центрах валидации;
- метод получения списка отозванных сертификатов (CRL) из точки распространения CRL для центра валидации;
- метод получения созданных точек распространения;
- метод получения параметров точки распространения по идентификатору;
- метод создания новой точки распространения;
- метод создания подключения точки распространения;
- метод удаления подключения точки распространения;
- метод редактирования параметров точки распространения;
- метод удаления точки распространения по ее идентификатору;
- метод активации точки распространения;
- метод деактивации точки распространения;
- метод публикации данных в точку распространения по ее идентификатору;
- метод публикации данных в точки распространения;
- метод редактирования приоритета точки распространения;
- метод кластеризации точки распространения;
- метод генерации и публикации CRL в точки распространения по идентификатору центра сертификации;
- метод обновления CRL для списка центров сертификации;
- метод получения конфигурации CRL по идентификатору центра сертификации;
- метод редактирования конфигурации CRL по идентификатору центра сертификации;
- метод удаления конфигурации CRL по идентификатору центра сертификации;
- метод получения CRL по идентификатору центра сертификации;
- метод получения параметров CRL по идентификатору центра сертификации.

В составе серверной части Центра регистрации реализован программный интерфейс REST API, который предоставляет пользователю следующие методы:

- метод аутентификации x509 по сертификату безопасности;
- метод аутентификации пользователя в программе по Kerberos-ticket;
- метод аутентификации пользователя в программе по имени пользователя и паролю;
- метод выхода из аккаунта;
- метод идентификации и аутентификации пользователя по маркеру доступа в программе, предоставляет информацию о пользователе;
- метод генерации и предоставления нового маркера доступа при истечении срока действия текущего маркера доступа;
- метод получения информации о текущем пользователе;
- метод получения информации о сессиях пользователей;
- метод удаления сессий пользователей;
- метод удаления сессии пользователя по идентификатору сессии;
- метод предоставления списка субъектов (получателей сертификатов);
- метод предоставления данных субъекта (получателя сертификатов) по его идентификатору;
- метод изменения статуса субъекта (получателя сертификатов).
- метод сохранения записи аудита в базу данных;
- метод получения записей аудита из базы данных;
- метод выставления метки об удалении учетной записи пользователя всем событиям в журнале;
- метод создания записи о новом syslog-сервере;
- метод редактирования записи о syslog-сервере;
- метод удаления записи о syslog-сервере;
- метод активации публикации сообщений с информацией о событиях аудита для syslog-сервера;
- метод выключения публикации сообщений с информацией о событиях аудита для syslog-сервера;
- метод получения списка созданных записей о syslog-серверах;
- метод получения данных Syslog-сервера по его идентификатору.
- метод создания новой заявки выпуска на ключевом носителе;
- метод создания новой заявки на основании запроса PKCS#10;
- метод создания новой заявки в формате WSTEP;
- метод создания новой заявки в формате SCEP;
- метод создания новой заявки на выпуск сертификата с закрытым ключом (PKCS#12) ;
- метод отзыва сертификата по идентификатору заявки;
- метод получения списка заявок;
- метод получения данных заявки по идентификатору;
- метод получения списка идентификаторов заявок;
- метод получения комментариев к заявке по ее идентификатору;
- метод получения статистики по заявкам;

- метод получения связанных с заявкой файлов по идентификатору заявки;
- метод получения данных заявки по внешнему ключу;
- метод запуска выполнения правила для заявок;
- метод запуска выполнения правила для заявки по ее идентификатору;
- метод получения списка доступных правил для заявки по ее идентификатору.
- метод установки контейнера закрытого ключа и сертификата веб-сервера операционной системы (среды функционирования);
- метод предоставления данных текущего сертификата веб-сервера операционной системы (среды функционирования);
- метод предоставления информации о программе;
- метод синхронизации издателей сертификатов доступа с центром сертификации;
- метод активации издателей сертификатов доступа;
- метод получения списка разрешенных издателей сертификатов доступа;
- метод предоставления списка доступных пользователю страниц веб-интерфейса в соответствии с его ролью.
- метод получения файлов из хранилища;
- метод сохранения файлов в хранилище;
- метод удаления файлов из хранилища;
- метод получения файла из хранилища с выбранным идентификатором.
- метод создания новой политики обработки заявки;
- метод копирования политики обработки заявки;
- метод редактирования политики обработки заявки;
- метод редактирования состояния политики обработки заявки;
- метод получения списка политик обработки заявок;
- метод получения политики обработки заявки по ее идентификатору;
- метод получения шаблона политики обработки заявки для субъекта;
- метод получения списка всех доступных шаблонов политик обработки заявок;
- метод удаления политики обработки заявки по ее идентификатору;
- метод удаления целей для политик обработки заявки;
- метод удаления цели для политики обработки заявки;
- метод удаления источников для политик обработки заявки;
- метод удаления источника для политики обработки заявки;
- метод создания новой SCEP-политики;
- метод изменения состояния SCEP-политики;
- метод редактирования SCEP-политики;
- метод получения списка SCEP-политик;
- метод получения SCEP-политики обработки заявки по ее идентификатору;

- метод удаления SCEP-политики обработки заявки по ее идентификатору.
- метод экспорта файла запроса на сертификат по идентификатору заявки;
- метод экспорта файла контейнера закрытого ключа по идентификатору заявки;
- метод экспорта файла списка отозванных сертификатов (CRL) издателя по идентификатору заявки;
- метод экспорта файла цепочки сертификатов по идентификатору заявки;
- метод экспорта файла цепочки сертификатов издателя по идентификатору заявки;
- метод экспорта файла сертификата по идентификатору заявки;
- метод экспорта файла сертификата издателя по идентификатору заявки;
- метод экспорта файла цепочки сертификатов по идентификатору центра сертификации;
- метод создания задачи по формированию файла, содержащего в себе записи аудита из хранилища программы;
- метод повторного запуска задачи по формированию файла, содержащего в себе записи аудита или данные сертификатов;
- метод экспорта (по идентификатору задачи) файлов с записями о событиях аудита;
- метод получения информации о задаче по формированию файлов с записями о событиях аудита или данными сертификатов.
- метод получения списка шаблонов сертификатов;
- метод получения шаблона сертификата по его идентификатору;
- метод обновления активности учетной записи по ее идентификатору;
- метод получения списка учетных записей;
- метод получения данных учетной записи по ее идентификатору;
- метод получения данных учетной записи по отпечатку сертификата;
- метод получения списка центров сертификации;
- метод предназначен получения данных центра сертификации по его идентификатору;
- метод получения данных текущего центра сертификации;
- метод получения данных активного центра сертификации;
- метод выпуска сертификата по запросу для центра сертификации;
- метод выпуска сертификата с закрытым ключом для центра сертификации;
- метод перевыпуска сертификата по запросу для центра сертификации;
- метод отзыва сертификата по его идентификатору;
- метод получения сертификата по его идентификатору;
- метод получения сертификата по его отпечатку;
- метод получения файла запроса на сертификат по идентификатору сертификата;
- метод получения файла контейнера PKCS#12 по идентификатору сертификата;
- метод получения файла цепочки сертификатов по идентификатору сертификата;
- метод получения файла сертификата по его идентификатору;
- метод получения файла CRL по идентификатору центра сертификации;

- метод получения файла цепочки сертификатов по идентификатору центра сертификации;
- метод получения файла сертификата по идентификатору центра сертификации;
- метод расшифрования контейнера закрытого ключа;
- метод расшифрования контейнера сертификата;
- метод расшифрования сертификата;
- метод обновления (создания) субъекта;
- метод обновления (создания) субъекта на основании запроса PKCS#10;
- метод получения списка субъектов;
- метод получения данных субъекта по его идентификатору;
- метод получения списка идентификаторов субъектов;
- метод получения списка издателей.
- метод получения списка шаблонов сертификатов;
- метод получения шаблона сертификата по его идентификатору;
- метод получения списка доступных шаблонов сертификатов;
- метод получения списка учетных записей;
- метод получения данных учетной записи по ее идентификатору;
- метод получения списка центров сертификации;
- метод получения данных центра сертификации по его идентификатору;
- метод получения данных текущего центра сертификации;
- метод получения списка политик обработки заявок;
- метод получения политики обработки заявки по ее идентификатору;
- метод получения списка SCEP-политик;
- метод получения SCEP-политики обработки заявки по ее идентификатору;
- метод получения сертификата по идентификатору заявки.
- метод создания нового SCEP-профиля;
- метод активации SCEP-профиля;
- метод остановки SCEP-профиля;
- метод поиска SCEP-профилей;
- метод поиска SCEP-профиля по его идентификатору;
- метод удаления SCEP-профиля;
- метод GET-операций по протоколу SCEP;
- метод POST-операций по протоколу SCEP.
- метод обработки запросов по протоколу WSTEP.

В составе серверной части Центра валидации реализован программный интерфейс REST API, который предоставляет пользователю следующие методы:

- метод аутентификации x509 по сертификату безопасности;
- метод аутентификации пользователя в программе по Kerberos-ticket;

– метод аутентификации пользователя в программе по имени пользователя и паролю;

– метод авторизации под локальной учетной записью;

– метод выхода из аккаунта;

– метод идентификации и аутентификации пользователя по маркеру доступа в программе, предоставляет информацию о пользователе;

– метод генерации и предоставления нового маркера доступа при истечении срока действия текущего маркера доступа;

– метод получения текущего пользователя;

– метод создания локальной учетной записи;

– метод поиска (получения информации) о локальных учетных записях;

– метод обновления пароля локальной учетной записи;

– метод получения информации о сессиях пользователей;

– метод удаления сессий пользователей;

– метод удаления сессии пользователя по идентификатору сессии.

– метод сохранения записи аудита в базу данных;

– метод получения записей аудита из базы данных;

– метод выставления метки об удалении учетной записи пользователя всем событиям в журнале;

– метод создания записи о новом syslog-сервере;

– метод редактирования записи о syslog-сервере;

– метод удаления записи о syslog-сервере;

– метод активации публикации сообщений с информацией о событиях аудита для syslog-сервера;

– метод выключения публикации сообщений с информацией о событиях аудита для syslog-сервера;

– метод получения списка созданных записей о syslog-серверах;

– метод получения данных Syslog-сервера по его идентификатору.

– метод установки контейнера закрытого ключа и сертификата веб-сервера операционной системы (среды функционирования);

– метод предоставления данных текущего сертификата веб-сервера операционной системы (среды функционирования);

– метод предоставления информации о программе;

– метод запуска процесса инициализации программы;

– метод синхронизации издателей сертификатов доступа с центром сертификации;

– метод активации издателей сертификатов доступа;

– метод получения списка разрешенных издателей сертификатов доступа;

– метод предоставления списка доступных пользователю страниц веб-интерфейса в соответствии с его ролью.

– метод получения файлов из хранилища;

– метод сохранения файлов в хранилище;

- метод удаления файлов из хранилища;
- метод получения файла из хранилища с выбранным идентификатором.
- метод создания нового центра валидации;
- метод проверки доступности центра валидации;
- метод переподключения центра валидации;
- метод получения информации по идентификатору о центре валидации;
- метод получения списка центров валидации;
- метод удаления по идентификатору центра валидации;
- метод запуска службы OCSP;
- метод остановки службы OCSP;
- метод обновления параметров службы OCSP;
- метод перепуска сертификата службы OCSP;
- метод получения параметров службы OCSP;
- метод получения сертификата службы OCSP;
- метод удаления по идентификатору службы OCSP;
- метод создания службы OCSP;
- метод обработки OCSP-запроса;
- метод получения службы OCSP;
- метод получения информации о службе OCSP;
- метод загрузки сертификата текущего издающего центра сертификации (AIA) в точку распространения CRL;
- метод получения опубликованного сертификата текущего издающего центра сертификации (AIA) из точки распространения CRL;
- метод получения информации об опубликованном сертификате текущего издающего центра сертификации (AIA);
- метод загрузки списка отозванных сертификатов (CRL) в точки распространения (CDP)
- метод загрузки Delta CRL в точки распространения (CDP);
- метод получения списка отозванных сертификатов (CRL) из точки распространения (CDP);
- метод получения Delta CRL из точки распространения (CDP);
- метод получения информации о списке отозванных сертификатов (CRL) из точки распространения (CDP);
- метод получения информации о Delta CRL из точки распространения (CDP).
- метод получения списка шаблонов сертификатов;
- метод получения шаблона сертификата по его идентификатору;
- метод проверки доступности центра валидации;
- метод создания центра валидации;
- метод удаления центра валидации;

- метод обновления активности учетной записи по идентификатору;
- метод получения списка учетных записей;
- метод получения данных учетной записи по ее идентификатору;
- метод получения данных учетной записи по идентификатору субъекта;
- метод получения данных учетной записи по отпечатку сертификата;
- метод получения списка центров сертификации;
- метод получения данных центра сертификации по его идентификатору;
- метод получения данных текущего центра сертификации;
- метод создания службы OCSP;
- метод удаления службы OCSP по идентификатору центра валидации;
- метод получения данных активного центра сертификации;
- метод добавления подключения к центру сертификации;
- метод получения списка подключений к центрам сертификации;
- метод получения информации о подключениях центрам сертификации;
- метод удаления подключения (по идентификатору) к центру сертификации;
- метод выпуска сертификата по запросу для центра сертификации;
- метод выпуска сертификата с закрытым ключом для центра сертификации;
- метод перевыпуска сертификата по запросу для центра сертификации;
- метод отзыва сертификата по его идентификатору;
- метод получения сертификата по его идентификатору;
- метод получения сертификата по его отпечатку;
- метод получения файла запроса на сертификат по идентификатору сертификата;
- метод получения файла закрытого ключа по идентификатору сертификата;
- метод получения файла цепочки сертификатов по идентификатору сертификата;
- метод получения файла сертификата по его идентификатору;
- метод получения файла CRL по идентификатору центра сертификации;
- метод получения файла цепочки сертификатов по идентификатору центра сертификации;
- метод получения файла сертификата по идентификатору центра сертификации
- метод расшифрования контейнера закрытого ключа;
- метод расшифрования сертификата;
- метод расшифрования контейнера сертификата;
- метод предоставления списка субъектов ресурсных систем;
- метод предоставления данных субъекта по его идентификатору;
- метод предоставления списка идентификаторов субъектов;
- метод обновления (создания) субъекта;
- метод обновления (создания) субъекта на основании запроса pkcs#10;
- метод получения списка издателей.

2 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ «КРИПТОПРО CSP» В СОСТАВЕ ПРОГРАММНОГО СРЕДСТВА

Программное средство использует следующие функции СКЗИ «КриптоПро CSP»:

- генерация закрытых и открытых ключей обмена в соответствии с ГОСТ Р 34.10-2012;
- работа с сертификатами открытых ключей по X.509;
- хэширование данных в соответствии с ГОСТ Р 34.11-2012;
- формирование электронной цифровой подписи в соответствии с ГОСТ Р 34.10-2012;
- проверка электронной цифровой подписи в соответствии с ГОСТ Р 34.10-2012;
- защита от НСД ключевой информации;
- установление соединений по TLS с использованием отечественных криптографических алгоритмов.

Использование СКЗИ «КриптоПро CSP» Версия 5.0 R3 КС1 (исполнение 1-Base) должно выполнятся в соответствии с документом «СКЗИ «КриптоПро CSP». Правила пользования» ЖТЯИ.00101-03 95 01 [1].

Использование СКЗИ «КриптоПро CSP» Версия 5.0 R3 КС2 (исполнение 2-Base) должно выполнятся в соответствии с документом «СКЗИ «КриптоПро CSP. Правила пользования» ЖТЯИ.00102-03 95 01 [2].

Организация работ по защите от НСД СКЗИ «КриптоПро CSP», ключевой и защищаемой информации должна выполняться в соответствии требованиями п.5.1, 5.4 [1], [2].

Размещение технических средств с установленным СКЗИ «КриптоПро CSP» должно выполняться в соответствии с п.5.2 документов [1] и [2].

Установка системного и прикладного, специального ПО и СКЗИ «КриптоПро CSP» должны выполняться в соответствии с п.5.3 документов [1] и [2].

Эксплуатация СКЗИ «КриптоПро CSP» должна выполняться в соответствии с п.6, п.4.5 документов [1] и [2].

Использование ключевых носителей СКЗИ «КриптоПро CSP» должно выполняться в соответствии с п.3.3 документов [1] и [2].

Хранение ключевой информации и ключевых носителей СКЗИ «КриптоПро CSP» должно выполняться в соответствии с п.3.8 документов [1] и [2].

Сроки использования ключевой информации СКЗИ «КриптоПро CSP» должны устанавливаться в соответствии с п.3.7 документов [1] и [2].

Управление ключевой информацией СКЗИ «КриптоПро CSP» должно выполняться в соответствии с п.3.10 документов [1] и [2].

Резервное копирование ключевой информацией и хранение резервных копий ключей СКЗИ «КриптоПро CSP» должно выполняться в соответствии с п.5.6 документов [1] и [2].

Контролем целостности должны быть охвачены файлы, указанные в разделе «Требования по криптографической защите» документов «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03 [3] и «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00102-03 91 03 [4].

Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам должен быть Администратор безопасности. Порядок подключения СКЗИ к каналам определен в документах [5]-[7]. Иные способы подключения к каналам связи запрещены.

При подключении Администратором безопасности должен быть обеспечен организационно-технический контроль запросов на установление соединения абонентов по протоколу TLS с использованием эфемерных ключей, исключающих возможность использования абонентом не своих атрибутов соединения (такие, как Client_Id и т.п.).

3 ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ ОБЬЕКТОВ

В перечень объектов, защищаемых от несанкционированного доступа и модификации, входят:

– Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также его состав (п.1.2 настоящего Руководства);

– Аппаратные средства, на которых осуществляется функционирование серверного компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также их состав (п.1.4 настоящего Руководства);

– Общесистемное ПО (ОС), в среде которого осуществляется функционирование серверного компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также его состав (п.1.4 настоящего Руководства);

– Прикладное ПО (СУБД, Веб-сервер, Среда разработки и исполнения), совместно с которым осуществляется функционирование серверного компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также его состав (п.1.4 настоящего Руководства);

– СКЗИ и специальное ПО, входящее в его состав (п.1.4 настоящего Руководства);

– Аппаратные средства, на которых осуществляется функционирование клиентского компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также их состав (п.1.4 настоящего Руководства);

– Общесистемное ПО (ОС), в среде которого осуществляется функционирование клиентского компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также его состав (п.1.4 настоящего Руководства);

– Прикладное ПО (веб-браузер), совместно с которым осуществляется функционирование клиентского компонента программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также его состав (п.1.4 настоящего Руководства).

4 ТРЕБОВАНИЯ К НАСТРОЙКАМ БЕЗОПАСНОСТИ

Использование СКЗИ «КриптоПро CSP» с выключенным режимом усиленного контроля использования ключей не допускается.

Настройки ОС для работы с СКЗИ должны производиться в соответствии с документом «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03 [3] и документом «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00102-03 91 03 [4]. Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

– на ПЭВМ должна быть установлена только одна операционная система. При использовании СКЗИ «КриптоПро CSP» исполнения 1-Base в случае использования виртуальной инфраструктуры допускается установка одной хостовой и неограниченного числа гостевых ОС. При использовании СКЗИ «КриптоПро CSP» исполнения 2-Base – использование виртуализации запрещено;

– в системе регистрируется один пользователь, обладающий правами администратора, на которого возлагается обязанность конфигурировать ОС, настраивать безопасность ОС, а также конфигурировать ПЭВМ, на которую установлена ОС;

– правом установки и настройки ОС и СКЗИ должен обладать только Администратор безопасности;

– все неиспользуемые ресурсы системы необходимо удалить или отключить (протоколы, сервисы, порты, общие ресурсы, пользователи и т.п.);

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в ОС, Администратор безопасности в соответствии с политикой безопасности, принятой в организации, даёт минимально возможные для нормальной работы права; каждый пользователь ОС, не являющийся администратором, может просматривать и редактировать только свои настройки в рамках прав доступа, назначенных ему администратором;

– необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

  – системный реестр;
  – файлы и каталоги;
  – временные файлы;
  – журналы системы;
  – файлы подкачки;
  – кэшируемая информация (пароли и т.п.);
  – отладочная информация.

– кроме того, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ (если это не выполнимо, то на жёсткий диск должны распространяться требования, предъявляемые к ключевым носителям);

– должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию;

– средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты (POST);

– средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств и PCI-устройств;

– в случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносного ПО, загружаемых из сети;

– при использовании СКЗИ на ПЭВМ/устройствах, подключённых к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, IPS/IDS, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

5 ТРЕБОВАНИЯ ПО УСТРАНЕНИЮ ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ

В целях противодействия негативному влиянию со стороны совместно функционирующего ПО на программное средство в условиях возможного возникновения уязвимостей запрещается использование в составе совместно функционирующего ПО нелицензионного программного обеспечения. Для используемого лицензионного ПО необходимо периодически (рекомендуемая частота – 1 раз неделю) проводить поиск уязвимостей по общедоступным базам. При закрытии уязвимости обновлением (патчем) выполняется его применение. При отсутствии в общедоступной базе способа противодействия выявленным уязвимостям (в период отсутствия обновления/патча) использование программного средства запрещается. по решению Администратора безопасности допускается не прекращать функционирование программного средства при наличии обоснования отсутствия негативного влияния выявленной уязвимости на функционирование программного средства. Контроль наличия обновлений и их применение должны проводится независимо от контроля наличия уязвимостей (рекомендуемая частота – 1 раз неделю).

6 ОБЪЕКТЫ И РЕГЛАМЕНТ ПРОВЕДЕНИЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ

После загрузки ОС должен выполняться стартовый (сразу после загрузки) и периодический (один раз в неделю) контроль целостности ПО, входящего в состав СКЗИ, ОС, прикладного ПО и ПО программного средства (состав приведен в п.1.4 настоящего Руководства) с использованием утилиты «cpverify». Возможно использование утилиты «jcverify» из состава программного средства. Если проверка целостности перечисленных компонентов завершается ошибкой, Администратор безопасности должен выявить причину и обстоятельства нарушения целостности ПО и переустановить ПО в соответствии с инструкцией по установке, описанной в Руководстве администратора безопасности для используемой программно-аппаратной платформы.

При использовании СКЗИ «КриптоПро CSP» исполнения 2-Base дополнительно должен быть реализован контроль целостности перечисленных объектов ПО с использованием модуля доверенной загрузки. Контроль должен выполняться до загрузки ОС.

7 ТРЕБОВАНИЯ К НАСТРОЙКАМ И ПРОВЕДЕНИЮ АУДИТА

Для обеспечения проведения аудита событий безопасности Администратору Безопасности необходимо:

– выполнить настройку средств регистрации событий программного средства в соответствии с документами [5]-[7];

– выполнить настройку компонентов ОС, отвечающих за ведение журналов событий, обеспечив выполнение режима архивирования журнала при его заполнении.

Администратору Безопасности необходимо организовать и проводить регулярный анализ результатов аудита.

8 ТРЕБОВАНИЯ К НАСТРОЙКАМ СЕТЕВОГО ДОСТУПА К КОМПОНЕНТАМ ПРОДУКТА

Для обеспечения необходимого уровня информационной безопасности при сетевом доступе к программному средству должны выполняться следующие требования:

– для защиты канала связи при сетевом доступе к программному средству необходимо использовать средства, сертифицированные ФСБ России по классу КС1 (при использовании СКЗИ «КриптоПро CSP» исполнения 1-Base) либо по классу КС2 (при использовании СКЗИ «КриптоПро CSP» исполнения 2-Base);

– для защиты канала связи между серверным и клиентским компонентами программного средства необходимо использовать СКЗИ, сертифицированные ФСБ России по классу КС1 (при использовании СКЗИ «КриптоПро CSP» исполнения 1-Base) либо по классу КС2 (при использовании СКЗИ «КриптоПро CSP» исполнения 2-Base) и реализующие защиту канала по протоколу TLS с использованием криптографических алгоритмов, определенных в государственных стандартах и действующих методических рекомендациях;

– необходимо исключить возможность удаленного управления, администрирования и модификации ОС, прикладного ПО и аппаратных средств серверного и клиентского компонентов программного средства.

9 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ВВОДЕ ПРОГРАММНОГО СРЕДСТВА В ЭКСПЛУАТАЦИЮ

При вводе в эксплуатацию программного средства должна быть обеспечена защита аппаратного и программного обеспечения программного средства от НСД. При размещении технических средств программного средства:

– Должны быть приняты меры по исключению несанкционированного доступа к ПЭВМ/устройствам, на которых установлено программное средство, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе с указанными ПЭВМ/устройствами. В случае такой необходимости должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на ПЭВМ/устройства, на которых эксплуатируется программное средство, и защищаемую информацию.

– Должны быть приняты меры по исключению возможности доступа неавторизованного персонала к консоли, системе питания и дополнительным устройствам, подключенным к защищаемому серверу путём установки оборудования в специально выделенное и запираемое помещение (аппаратную или серверную комнату). Доступ персонала в серверную комнату должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

– Должны быть приняты меры, исключающие несанкционированное вскрытие корпусов ПЭВМ, устройств и средств, входящих в состав СФ программного средства.

– Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях, в которых расположены ПЭВМ с установленным программным средством, должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

– Размещение программного средства в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

– Размещение аппаратно-программных компонентов, являющихся средой функционирования СУБД (при ее развертывании на отдельном хосте), кластеров (как виртуальных, так и физических) и программно-аппаратного криптографического модуля «КриптоПро HSM» должно выполняться в пределах одной контролируемой зоны.

– Для исключения сбоев компьютера, вызванных отключением электропитания, необходимо обеспечить электропитание сервера от источника бесперебойного питания достаточной мощности. Как минимум, мощности батарей источника бесперебойного питания должно хватать на время достаточное для корректного автоматического завершения работы сервера.

При вводе в эксплуатацию программного средства должны быть выполнены следующие требования по обеспечению безопасности информации:

– Для аппаратных компонентов, на которых функционирует программное средство, должны быть проведены проверки ПО BIOS на соответствие методическим документам ФСБ России в области исследований программного обеспечения BIOS.

– При использовании СКЗИ «КриптоПро CSP» исполнения 2-Base должны быть выполнены процедуры установки и настройки средств доверенной загрузки, обладающих сертификатом ФСБ России.

– Для программных компонентов должна быть выполнена установка, конфигурация и настройка в соответствии с требованиями документов [5]-[7].

– При установке, конфигурации и настройке программного средства должен быть выполнен выбор криптографических алгоритмов в соответствии с правилами пользования [1] и [2].

– Политика реализации парольной защиты информации должна обеспечивать выполнение следующих требований:

  – парольная защита должна обеспечивать разграничение доступа на следующих рубежах: при запуске ОС, при входе в BIOS, при доступе к ключевой информации, при доступе к конфигурированию и использованию функций прикладного ПО, конфигурированию и использованию функций программного средства;
  – парольная защита при запуске ОС, при входе в BIOS, при доступе к ключевой информации, при доступе к конфигурированию и использованию функций прикладного ПО, конфигурированию и использованию функций программного средства должна осуществлять с использованием независимых паролей;
  – запрещено сохранять пароли, в том числе с использованием средств ОС, прикладного ПО и программного средства. Запрещено записывать пароли, в том числе с целью облегчения процесса эксплуатации.
  – парольная защита должна обеспечивать правила задания, смены и обращения с паролями в соответствии с п.5.4 [1], [2].
  – политика парольной защиты обязательна для всех учётных записей, зарегистрированных в программном средстве;
  – при использовании СКЗИ «КриптоПро CSP» исполнения 2-Base в дополнение к парольной защите должен использоваться механизм разграничения доступа, реализуемый используемым средством доверенной загрузки.

– При установке, конфигурации и настройке средств защиты канала (веб-сервер «cpnginx» из состава СКЗИ «КриптоПро CSP») должен быть выполнен выбор криптографических алгоритмов в соответствии с правилами пользования [1] и [2].

– При обработке с помощью программного средства конфиденциальной информации, передаваемой по каналам связи, выходящим за пределы контролируемой территории, необходимо использовать СКЗИ сертифицированные по классу не ниже КС1 (при использовании СКЗИ «КрпитоПро CSP» исполнения 1-Base) и по классу не ниже КС2 (при использовании СКЗИ «КрпитоПро CSP» исполнения 2-Base). При этом связь должна осуществляться по волоконно-оптическим линиям связи либо должны использоваться оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного фрагмента сети.

– Для программных компонентов должна быть исключена возможность неконтролируемого использования иных криптопровайдеров (кроме СКЗИ «КриптоПро CSP»);

– Администратор не должен иметь возможность доступа к конфиденциальной информации пользователей и операторов.

Администратор должен ознакомить каждого пользователя (оператора) программного средства с требованиями по безопасной эксплуатации программного средства.

10 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ ПРОГРАММНОГО СРЕДСТВА

При эксплуатации программного средства должна быть обеспечена защита аппаратного и программного обеспечения программного средства от НСД в объеме требований, предъявленных при вводе программного средства в эксплуатацию, в том числе:

– Должны соблюдаться меры по исключению несанкционированного доступа к ПЭВМ/устройствам, на которых установлено программное средство, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе с указанными ПЭВМ/устройствами. В случае такой необходимости должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на ПЭВМ/устройства, на которых эксплуатируется программное средство, и защищаемую информацию.

– Должны обеспечиваться меры, исключающие несанкционированное вскрытие корпусов ПЭВМ, устройств и средств, входящих в состав СФ программного средства.

Требования по защите от несанкционированного доступа к аппаратно-программным средствам и ключевой информации должны выполняться, в том числе, при выполнении технического обслуживания, при передаче в ремонт и в других случаях, когда возможна компрометация ключевой информации.

Администратор не должен иметь возможность доступа к конфиденциальной информации пользователей.

Администратор должен периодически проводить проверку знания операторами программного средства требований по его безопасной эксплуатации.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЦС – центр сертификации
CRL – список отозванных сертификатов
ОС – операционная система
СУБД – система управления базами данных
СКЗИ – средство криптографической защиты информации
REST-API – интерфейс сетевого взаимодействия программ
pkcs#12 – стандарт инфраструктуры Public-Key Cryptography
pkcs#10 – стандарт инфраструктуры Public-Key Cryptography
X.509– стандарт инфраструктуры Public-Key Cryptography
НСД – несанкционированный доступ
TLS – протокол криптографически защищенного обмена
ПО – программное обеспечение
ППО – прикладное программное обеспечение
SESPAKE - протокол выработки общего ключа с аутентификацией на основе пароля
ПЭВМ – персональная электронная вычислительная машина
USB – последовательный стык
ЭП – электронная подпись
АС – аппаратные средства
СФ – среда функционирования
POST – автоматическая проверка исправности ПЭВМ x86 архитектуры
BIOS – базовая система ввода/вывода ПЭВМ x86 архитектуры
МДЗ- модуль доверенной загрузки
ФСБ – Федеральная Служба Безопасности

СПИСОК ЛИТЕРАТУРЫ

1. ЖТЯИ.00101-03 95 01. СКЗИ «КриптоПро CSP». Правила пользования.
2. ЖТЯИ.00102-03 95 01. СКЗИ «КриптоПро CSP». Правила пользования.
3. ЖТЯИ.00101-03 91 03 СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.
4. ЖТЯИ.00102-03 91 03 СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux.
5. RU.АЛДЕ.03.01.020 32 01-1 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority/
6. RU.АЛДЕ.03.01.020 32 01-4. Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority.
7. RU.АЛДЕ.03.01.020 32 01-5. Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 5. Центр регистрации Aladdin Enterprise Registration Authority.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					