УТВЕРЖДАЮ
Директор республиканского унитарного предприятия «Национальный центр электронных услуг»

_____ А.А. Ильин

«__30__» ____12_____ 2016 г.

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ
республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

Минск
2016

СОДЕРЖАНИЕ

1. Введение в регламент деятельности

1.1. Общие положения

Настоящий регламент деятельности по применению сертификатов открытых ключей (далее – Регламент) республиканского удостоверяющего центра (далее – РУЦ) Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) является долговременным документом, содержащим описание системы и практики работы РУЦ с сертификатами открытых ключей (далее – сертификат) и списками отозванных сертификатов (далее – СОС), регламентирует операционную работу РУЦ, а также регулирует ответственность пользователей при получении и использовании сертификатов и личных ключей подписи.

Регламент разработан в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров» и устанавливает совокупность правил, определяющих порядок действий РУЦ при издании, управлении, отзыве и обновлении сертификатов и СОС.

Для целей настоящего Регламента термины и их определения используются в значениях, установленных Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» (Национальный реестр правовых актов Республики Беларусь, 2010 г., № 15, 2/1665), Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» (Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225), Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10.12.2015 № 118 (Национальный правовой Интернет-портал Республики Беларусь, 10.12.2015, № 7/3335) (далее – Положение), техническими нормативными правовыми актами, государственным стандартом Республики Беларусь СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров» и другими техническими нормативными правовыми актами.

В соответствии с Положением ГосСУОК строится как иерархическая инфраструктура открытых ключей и состоит из корневого удостоверяющего центра, подчиненного ему РУЦ и регистрационных центров (далее – РЦ).

Основными функциями РУЦ являются:

генерация личных и открытых ключей РУЦ;

издание, распространение, предоставление информации о статусе, отзыв и хранение сертификатов регистраторов РУЦ и РЦ (далее - регистратор), центра атрибутных сертификатов, физических и юридических лиц, сервисов (приложения, серверы или устройства);

удостоверение формы внешнего представления электронных документов на бумажном носителе;

функции РЦ.

РУЦ осуществляет согласование регламентов работы и инструктаж персонала РЦ, присоединившихся к ППС РУЦ.

В соответствии с Указом Президента Республики Беларусь от 23 января 2014 г. № 46 (Национальный правовой Интернет-портал Республики Беларусь, 27.01.2014, № 1/14787) функции оператора РУЦ (далее - Оператор) осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее – НЦЭУ).

Юридический адрес:

Республика Беларусь, 220004, г. Минск, ул. Раковская, 14.

Банковские реквизиты:

Расчетный счет 3012089370084 филиал № 529 «Белсвязь» ОАО «АСБ Беларусбанк» МФО 153001720, 220005 г. Минск, пр. Независимости, 56.

УНП 191700161.

Адрес местонахождения:

Республика Беларусь, 220002, г. Минск, пр. Машерова, 25-200.

Контактные телефоны, факс, адрес электронной почты и Интернет-сайта Оператора:

телефон:	(017) 229 30 00;
факс:	(017) 229 30 06;
e-mail:	pkigov@nces.by
адрес Интернет-сайта:	http://nces.by

1.2. Пользователи регламента

Пользователями Регламента являются пользователи сертификатов (доверяющие стороны, далее – пользователи).

Сертификаты, изданные в соответствии с настоящим Регламентом могут быть использованы для целей, определенных соответствующей политикой применения сертификатов РУЦ ГосСУОК (далее - ППС).

Настоящий Регламент не ограничивает использование данных сертификатов никакими программными приложениями.

2. Требования к участникам ГосСУОК

2.1. Требования к РУЦ

РУЦ осуществляет свою деятельность в соответствии с Положением и выполняет все требования, установленные в разделах 3 ППС и настоящего Регламента.

Оператор несет ответственность за соответствие процедурам, установленным настоящим Регламентом, в соответствии с законодательством Республики Беларусь.

Положения Регламента могут уточняться в ППС.

2.2. Требования к РЦ

РЦ соответствии с Положением осуществляет проверку информации, вносимой в сертификат, формирование заявок на издание и отзыв сертификата, передачу конечным пользователям изданных сертификатов, обеспечение их взаимодействия с РУЦ.

При формировании заявки на и (или) отзыв сертификата РЦ должен установить и достоверно подтвердить личность физического лица (данные о государственной регистрации юридического лица), а также полноту и точность представленных идентификационных данных согласно ППС РУЦ и регламенту РЦ.

РЦ осуществляют свою деятельность в соответствии с ППС, настоящим Регламентом и регламентом работы, согласованным с РУЦ.

2.3. Требования к подписчикам

Подписчиком может являться ФЛ или юридическое лицо.

Подписчик должен:

гарантировать, что вся информация, предоставляемая для издания и использования его открытого ключа и сертификата, является полной и точной;

использовать личный и открытый ключи только для выработки и проверки ЭЦП соответственно, а также в соответствии с любыми другими ограничениями, о которых уведомляется подписчик;

осуществлять выработку личного ключа и открытого ключа с использованием средства ЭЦП, имеющего сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь;

хранить в тайне личный ключ;

обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);

отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена.

не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия такого открытого ключа истек.

В случае, если подписчик и субъект являются разными лицами, подписчик должен информировать субъекта о данных требованиях.

2.4. Требования к доверяющей стороне

Перед установлением доверия к электронному документу, в частности сертификату, доверяющая сторона должна:

убедиться в действительности сертификата, включая его проверку на отзыв или истечение срока действия;

удостовериться, что назначение сертификата соответствует предполагаемой области применения и любым другим ограничениям, связанным с его использованием, которые указаны в нем или в соответствующей ППС.

3. Требования к РУЦ

3.1. Требования по управлению ключами

3.1.1. Выработка личного ключа РУЦ

Выработка личного ключа и открытого ключа РУЦ осуществляется подготовленными и доверенными работниками Оператора в конструктивно защищенной среде под контролем как минимум двух работников Оператора с использованием сертифицированного программно-аппаратного средства электронной цифровой подписи (далее – ЭЦП), имеющего сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь.

Порядок выработки личного ключа подписи и формирование запроса к корневому УЦ на издание сертификата РУЦ определен во внутреннем документе Оператора.

Срок действия сертификата РУЦ определен в ППС РУЦ.

До истечения срока действия личного ключа подписи РУЦ *(validity сертификата РУЦ – validity максимальный срок действия издаваемых РУЦ сертификатов конечного пользователя)* Оператор вырабатывает новую пару ключей для подписи издаваемых сертификатов и принимает все необходимые меры для того, чтобы избежать нарушения деятельности любого участника, доверяющего сертификату РУЦ. Новые ключи РУЦ создаются и распространяются в соответствии с Регламентом.

3.1.2. Хранение, резервное копирование и восстановление личного ключа РУЦ

Личный ключ РУЦ хранится в тайне и используется только в сертифицированном программно-аппаратном средстве ЭЦП.

Средства контроля доступа к программно-аппаратному средству ЭЦП, в котором хранится личный ключ РУЦ, гарантируют отсутствие несанкционированного доступа к нему.

Работники РУЦ осуществляют резервное копирование личного ключа РУЦ. Резервная копия личного ключа РУЦ хранится в зашифрованном виде.

К ключу шифрования резервной копии личного ключа РУЦ применяется (5, 3) - пороговое разделение секрета в соответствии с криптографическим алгоритмом, установленным в СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета».

Резервное копирование личного ключа РУЦ и его восстановление осуществляется в присутствии как минимум двух подготовленных и доверенных работников РУЦ в отдельном помещении на программно-аппаратном средстве ЭЦП под контролем комиссии (владельцы частичных секретов резервной копии личного ключа РУЦ различны).

Безопасность резервных копий личного ключа РУЦ обеспечивается на таком же или более высоком уровне, как и для постоянно используемого личного ключа РУЦ.

3.1.3. Распространение открытых ключей РУЦ

РУЦ распространяет свой открытый ключ в виде сертификата, подписанного личным ключом корневого удостоверяющего центра ГосСУОК.

Сертификаты РУЦ размещаются на Интернет-сайте Оператора.

Доверяющие стороны должны проводить проверку подлинности и целостности открытого ключа РУЦ при его получении.

3.1.4. Депонирование личного ключа РУЦ

РУЦ не осуществляет депонирование личного ключа РУЦ, несмотря на то, что он осуществляет его резервное копирование.

3.1.5. Использование личного ключа

РУЦ использует свой личный ключ только для издания сертификатов и СОС, определенных в соответствующей ППС.

3.1.6. Окончание срока действия личного ключа РУЦ

Личный ключ РУЦ не используется по окончании срока его действия.

Уничтожение копий личного ключа РУЦ без возможности восстановления все копии личного ключа РУЦ, в том числе и резервных, осуществляется после окончания срока его действия в порядке, определенном локальными нормативными актами Оператора.

3.1.7. Управление средством ЭЦП, используемым для издания сертификатов

В РУЦ для издания сертификатов и СОС используется программно-аппаратное средство ЭЦП, имеющее сертификат соответствия требованиям технического регламента Республики Беларусь ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность».

Оператор обеспечивает безопасность программно-аппаратного средства ЭЦП в течение всего срока его применения для издания сертификатов и СОС.

Оператор гарантирует, что:

программно-аппаратное средство ЭЦП не было повреждено во время поставки;

программно-аппаратное средство ЭЦП не было скомпрометировано во время хранения;

установка, активация, резервное копирование и восстановление личного ключа РУЦ в программно-аппаратном средстве ЭЦП проводится под контролем, как минимум двух доверенных работников оператора РУЦ и владельцев порогового числа частичных секретов, участвующих в восстановлении под контролем комиссии;

программно-аппаратное средство ЭЦП функционирует правильно;

личный ключ РУЦ, хранимый в программно-аппаратном средстве ЭЦП, уничтожается при изъятии данного средства из обращения.

3.2. Требования по управлению сертификатами

3.2.1. Регистрация владельца сертификата, издаваемого РУЦ

Регистрация владельца (субъекта) (физического лица или организации) для получения сертификата происходит в РУЦ и РЦ, аккредитованных в ГосСУОК.

При регистрации субъекта (физического лица или организации) для получения сертификата регистратор должен установить и достоверно подтвердить личность физического лица (подлинность организации), а также полноту и точность представленных идентификационных данных.

До вступления в договорные отношения с подписчиком, Оператор должен проинформировать его о нормах и правилах, касающихся использования сертификата, как установлено в 3.2.4.

При регистрации в соответствии с законодательством Республики Беларусь регистратор проверяет личность физического лица (подлинность организации) и другие необходимые для издания сертификата данные о лице (организации).

Личность физического лица проверяется на основании документа, удостоверяющего личность в соответствии с законодательством Республики Беларусь (информация, которая при этом подтверждается, – это фамилия и имя, дата рождения, идентификационный номер).

В случае, если субъектом является представитель юридического лица, проверка его подлинности осуществляется на основании следующей представленной информации:

полного имени (включая фамилию и имя), даты рождения, идентификационного номера уполномоченного лица;

полного наименования и правового статуса юридического лица;

иную регистрационную информацию о юридическом лице;

документы, подтверждающие связь субъекта с юридическим лицом.

В РУЦ (РЦ) регистрируется вся информация, используемая для проверки личности субъекта, включая номер документа, удостоверяющего

личность в соответствии с законодательством Республики Беларусь, дату выдачи данного документа, наименование органа, выдавшего его, а также другие данные.

Если подписчик, не являющийся субъектом, становится подписчиком услуг РУЦ (т.е. подписчик и субъект – отдельные участники), необходимо предоставить в РУЦ (РЦ) подтверждение того, что подписчик уполномочен осуществлять данную деятельность (т.е. подготовку необходимых документов на получение сертификатов для всех членов указанной организации формирует уполномоченное лицо).

Подписчик должен предоставить реквизиты адреса регистрации по месту жительства согласно правилам Всемирного почтового союза.

Регистратор должен зарегистрировать договор с подписчиком (сведения для регистрации), который включает:

права и обязанности подписчика (см. 2.3 настоящего Регламента);

согласие на то, чтобы РУЦ хранил информацию, предоставленную при регистрации, осуществлял любой последующий отзыв и передачу данной информации третьим сторонам на тех же условиях, какие требуются в соответствующей ППС в случае прекращения деятельности РУЦ;

согласие субъекта на опубликование сертификата и условия его публикации;

подтверждение того, что информация, содержащаяся в сертификате, является точной и полной.

Процесс формирования запроса на издание сертификата в РУЦ (РЦ) гарантирует, что субъект владеет личным ключом, связанным с открытым ключом, предоставленным для получения сертификата. Запрос на издание сертификата соответствует требованиям СТБ 34.101.17 – 2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».

подписчик вместе с запросом на издание сертификата представляет карточку открытого ключа в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи».

3.2.2. Возобновление действия сертификата и обновление данных

РУЦ осуществляет возобновление действия сертификата путем издания нового сертификата, сохранив без изменения информацию, содержащуюся в сертификате (кроме открытого ключа и срока действия сертификата), предварительно убедившись, что на момент обращения она является действительной.

подписчик может запросить обновление данных сертификата. Обновление данных осуществляется путем издания нового сертификата.

Регистратор убеждается, что информация, использованная для подтверждения личности и полномочий субъекта, на момент обращения является действительной.

Регистратор проверяет подлинность всей представленной подписчиком регистрационной информации в соответствии с порядком, установленным для первой регистрации.

РУЦ должен издавать новый сертификат, используя значение открытого ключа подписчика, содержащееся в предыдущем сертификате, только в случае, если его криптографическая стойкость не снизится за период действия нового сертификата и не существует признаков того, что личный ключ субъекта скомпрометирован.

3.2.3. Издание сертификата

РУЦ издает сертификат способом, обеспечивающим сохранение их подлинности и целостности.

Содержание полей сертификатов, издаваемых РУЦ, устанавливаются в соответствующей ППС. Формат сертификата соответствует СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

РУЦ гарантирует уникальность идентификационного номера сертификата.

Оператор РУЦ обеспечивает конфиденциальность и целостность регистрационных данных, передаваемых при обмене с подписчиком, субъектом или между компонентами автоматизированной информационной системы (далее - АИС) РУЦ.

В РУЦ проверяется подлинность и целостность представляемых РЦ регистрационных данных в электронном виде с помощью действительных сертификатов регистраторов.

На основании сертификата в порядке, установленном соответствующей ППС, может издаваться атрибутный сертификат (далее - АС), в котором определяются права (привилегии) владельца сертификата.

3.2.4. Распространение нормативных и организационных документов

Оператор гарантирует, что необходимые нормативные и организационные документы РУЦ являются доступными для подписчиков и доверяющих сторон РУЦ.

Оператор предоставляет доступ подписчикам и доверяющим сторонам к следующим нормативным и организационным документам:

копия лицензии на осуществление деятельности по оказанию услуг распространения открытых ключей проверки подписи;

копия аттестата об аккредитации РУЦ в ГосСУОК;

настоящий Регламент;

ППС;

порядок оказания электронных услуг РУЦ и аккредитованными РЦ;
адреса и контактные данные РУЦ и РЦ;
перечень информационных систем, использующих сертификаты РУЦ;
тексты публичных договоров на услуги РУЦ;
прейскурант тарифов на услуги РУЦ;
иные в документы, установленные в соответствующих ППС.

РУЦ предоставляет данную информацию с использованием долговечных носителей информации (т.е. сохраняющих целостность в течение длительного времени), в том числе в электронном виде, на государственном языке Республики Беларусь.

3.2.5. Распространение сертификатов

Сертификат подписчика становится действительным с даты начала действия, указанного в сертификате.

РУЦ (РЦ) размещает изданный сертификат подписчика на компакт-диск, который передается подписчику.

Изданный сертификат помещается в хранилище РУЦ и передается подписчику. По запросу подписчика или доверяющей стороны сертификат может быть отправлен по адресу электронной почты, указанному при регистрации.

Информация о назначении сертификата содержится в самом сертификате. Описание полей форматов сертификатов, издаваемых в РУЦ, описаны в приложении к соответствующей ППС.

Данная информация должна быть доступна 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от Оператора, Оператор принимает все необходимые меры, чтобы гарантировать, что данная услуга будет недоступна только в течение времени, установленного в соответствующей ППС.

3.2.6. Отзыв сертификата

Оператор гарантирует, что сертификат отзывается на основании запроса в сроки и в порядке, установленных в соответствующей ППС.

Оператор идентифицирует и проверяет запросы, связанные с отзывом сертификатов, на предмет их получения из достоверных источников.

Субъект и подписчик отозванного сертификата должны быть проинформированы Оператором об изменении статуса их сертификата.

Если сертификат отозван, он никогда не должен использоваться в дальнейшем.

3.2.7. Предоставление информации о статусе сертификата подписчика

При распространении РУЦ информации о статусе сертификата посредством издания СОС он издается и публикуется в реальном времени, а также:

каждый СОС издается не реже одного раза в месяц и содержит информацию о времени издания следующего СОС;

новый СОС может быть опубликован перед установленным временем издания следующего СОС;

СОС подписывается РУЦ;

формат СОС соответствует требованиям СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

Услуги РУЦ по управлению отзывом доступны в течение рабочего времени регистраторов, по получению статуса сертификата доступны 24 часа в сутки 365 дней в году. В случае отказа системы, сервисов или при наличии других факторов, не зависящих от Оператора, Оператор принимает все необходимые меры, чтобы гарантировать, что данная услуга будет недоступна только в течение времени, установленного в соответствующей ППС.

Информация о статусе сертификата должна быть доступна посредством размещения СОС на Интернет-сайте Оператора, а также через службу OCSP в соответствии с СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».

Информация об отзыве сертификата должна быть доступна по крайней мере до истечения срока действия данного СОС, установленного при его издании.

3.3. Управление деятельностью РУЦ

3.3.1. Управление безопасностью

Система защиты информации (далее – СЗИ) АИС РУЦ аттестована в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 «О некоторых вопросах технической и криптографической защита информации» (Национальный правовой Интернет-портал Республики Беларусь, 10.09.2013, 7/2561).

У Оператора принята Политика информационной безопасности, с которой ознакомлены все работники РУЦ, на которых она распространяется.

Требования к СЗИ АИС РУЦ уточняются при периодическом проведении оценки рисков. Оценка рисков выполняется с целью учета изменений в требованиях защиты и в рисковых ситуациях (активах, угрозах, слабых местах, негативных воздействиях, оценке значительности рисков, а также, когда происходят значительные изменения в СЗИ или АИС РУЦ). Работы по оценке рисков проводятся в сроки и порядке, определенном в Политике информационной безопасности РУЦ.

Оператор несет ответственность за все аспекты предоставления услуг по распространению открытых ключей.

3.3.2. Классификация и управление активами

Все критические активы РУЦ, требования и меры по их защите определены в задании по безопасности АИС РУЦ (далее – ЗБ АИС РУЦ), на предмет соответствия которого проведена аттестация системы защиты информации АИС РУЦ в реальных условиях эксплуатации.

В должностных инструкциях работников РУЦ определена их ответственность за поддержание основных мероприятий по управлению информационной безопасностью.

3.3.3. Вопросы безопасности, связанные с персоналом

На должности в РУЦ привлекаются работники Оператора, которые обладают необходимой квалификацией, опытом и прошли проверку на соответствие кадровой политике Оператора, что подтверждается внутренними локальными нормативными правовыми актами, регламентирующими деятельность РУЦ.

В должностных инструкциях работников Оператора определены их роли, права, обязанности и ответственность за обеспечение защиты информации. В них определены права и порядок доступа к защищаемой информации в соответствии с уровнем доступа к защищаемым сведениям, меры дисциплинарного воздействия, которые применяются в случае несанкционированных действий, нарушения политики информационной безопасности РУЦ.

Оператор повышает квалификацию своих работников в такой мере и с такой частотой, которые необходимы для обеспечения соответствующего уровня профессионализма, требуемого для исполнения их обязанностей надлежащим образом.

Работники Оператора, назначенные на доверенные должности, не имеют конфликта интересов, который может негативно повлиять на беспристрастность в их деятельности.

В РУЦ поддерживаются следующие роли работников с соответствующими обязанностями:

– администратор информационной безопасности: отвечает за администрирование СЗИ АИС РУЦ; осуществляет контроль целостности и подлинности текущих и архивных системных журналов событий и инцидентов безопасности АИС РУЦ, проведение аудита безопасности СЗИ АИС РУЦ;

– системный администратор: отвечают за установку, конфигурирование и обслуживание АИС РУЦ, используемых для регистрации, издания сертификата и управления отзывом; за повседневное обслуживание АИС РУЦ; осуществляет резервное копирование и восстановление АИС РУЦ;

– администратор баз данных: отвечает за управление, архивирование, резервное копирование и восстановление баз данных АИС РУЦ;

– регистратор: осуществляет проверку информации, вносимой в сертификаты, формирование заявок на издание и отзыв сертификатов, передачу конечным пользователям изданных сертификатов и карточек открытых ключей, обеспечение их взаимодействия с РУЦ.

Оператор не назначает на доверенные или управляющие должности лиц, которые имели судимости за серьезные преступления или другие преступления, которое могут повлиять на профессиональное выполнение служебных обязанностей. Работники Оператора не назначаются на доверенные должности, пока не завершены все необходимые проверки. Все работники Оператора проходят необходимые проверки в ОАЦ.

3.3.4. Физическая защита и защита от воздействий окружающей среды

Оператор обеспечивает физический доступ к оборудованию, используемому для изготовления и отзыва сертификатов, только уполномоченным лицам.

Оператор осуществляет контроль во избежание утери, повреждения или компрометации активов, которые могут привести к приостановлению его деятельности.

Оператор осуществляет контроль во избежание компрометации или кражи информации и оборудования, используемого для обработки этой информации.

Оператором создан серверный центр для реализации физически защищенной среды, которая обеспечивает обнаружение и предотвращение несанкционированного использования, доступа или разглашения информации, обрабатываемой в РУЦ. Безопасность серверного центра РУЦ проанализирована при проведении аттестации СЗИ АИС РУЦ и аккредитации РУЦ в ГосСУОК.

Любые лица, получающие физический доступ в серверный центр РУЦ, не должны оставаться там без надзора уполномоченного лица.

Оператором обеспечивается физическая защита помещений РУЦ и защита от воздействий окружающей среды для оборудования, используемого для реализации услуг РУЦ.

В локальных нормативных документах Оператора, разработанных в рамках реализации мероприятий по обеспечению информационной безопасности, описаны средства защиты всего оборудования РУЦ, включая конструкцию здания и размещение в нем помещений, физический доступ, электроснабжение и кондиционирование воздуха, построение телекоммуникационных кабельных сетей, противопожарные меры безопасности и защиты, хранение и утилизацию носителей информации, резервное копирование вне сети, техническое обслуживание оборудования, системы обнаружения физического вторжения и т.д.

3.3.5. Управление операционной деятельностью

АИС РУЦ и информация, обрабатываемая в АИС РУЦ, защищены от вирусов и недоверенного программного обеспечения.

В АИС РУЦ протоколируются все сбои и инциденты безопасности, а также СЗИ применяются меры быстрого реагирования на данные события.

В ЗБ АИС РУЦ определены процедуры, влияющие на предоставление услуг по распространению открытых ключей, политика управления носителями информации, используемыми в рамках деятельности РУЦ, для защиты их от повреждения, хищения и несанкционированного доступа к ним, а также политика по контролю журналов аудита АИС РУЦ на предмет наличия следов вредоносной деятельности.

Оператором определены и реализованы процедуры, влияющие на предоставление услуг по распространению открытых ключей, для всех доверенных и административных должностей.

Оператором проводятся мероприятия по обеспечению достаточности системных ресурсов и дискового пространства с целью обеспечения надлежащей обработки и хранения информации.

Оператором определены и применяются меры быстрого реагирования на все сбои и инциденты в работе СЗИ АИС РУЦ, а также на инциденты в области информационной и системной безопасности и ограничению влияния при нарушении безопасности.

В РУЦ процессы проверки, соответствия требованиям сохранности информации о сертификатов начинаются при запуске АИС РУЦ и заканчиваются при ее остановке.

В РУЦ операции по обеспечению безопасности отделены от любых других операций.

В политике информационной безопасности РУЦ и должностных инструкциях работников РУЦ определены обязанности по обеспечению безопасности РУЦ, которые включают рабочие процедуры и обязанности,

планирование системы защиты информации, мероприятия по обеспечению достаточности системных ресурсов и дискового пространства с целью обеспечения надлежащей обработки и хранения информации, защиту от вредоносного программного обеспечения, обеспечение безопасности помещений, сетевое управление, активное отслеживание журналов аудита, анализ событий и проверка исполнения, управление носителями информации и их безопасность, обмен данными и программным обеспечением.

3.3.6. Управление системным доступом

АИС РУЦ представляет собой информационную систему, на которой обрабатывается информация, охраняемая в соответствии с законодательством Республики Беларусь. Технические средства АИС РУЦ размещены в одной контролируемой зоне, и обработка защищаемой информации осуществляется в пределах области действия комплекса средств безопасности объекта.

В системе защиты информации АИС РУЦ применяются сертифицированные средства криптографической защиты информации для обеспечения конфиденциальности, контроля целостности (неизменности) и подлинности информации, распространение и (или) предоставление которой ограничено.

В АИС РУЦ управление доступом пользователей (включая регистраторов, администраторов и любых пользователей, имеющих прямой доступ к системе) к ресурсам, а также доступ к информации и системным функциям приложений ограничивается в соответствии с политикой информационной безопасности РУЦ.

В РУЦ ответственные работники перед использованием оборудования и программного обеспечения, связанного с управлением сертификатов и СОС, проходят процедуру двухфакторной идентификации и аутентификации.

Действия работников РУЦ и РЦ контролируются путем сохранения записей событий.

В АИС РУЦ информация, распространение и (или) предоставление которой ограничено, защищается, в том числе и на повторно используемых объектах хранения (например, удаленные файлы), доступных для неуполномоченных пользователей.

В АИС РУЦ локальные сетевые компоненты (например, маршрутизаторы) располагаются в физически безопасном окружении и их конфигурация периодически проверяется на соответствие требованиям, установленным в политике информационной безопасности РУЦ.

В помещениях, в которых размещены активы АИС РУЦ, организовано постоянное видеонаблюдение и установлены средства оповещения о тревоге, позволяющие иметь возможность соответствующим образом обнаруживать, регистрировать и реагировать на несанкционированные и ошибочные попытки доступа к данным активам.

3.3.7. Внедрение и обслуживание безопасных доверенных информационных систем

В АИС РУЦ используются безопасные доверенные информационные системы и продукты, которые защищены от модификации, и сертифицированные средства управления криптографическими ключами, сертификатов и СОС.

Анализ требований безопасности проводится на всех этапах разработки и эксплуатации информационных систем и продуктов, используемых в АИС РУЦ и обеспечивается необходимый уровень гарантии того, что в них надежно реализованы механизмы безопасности.

3.3.8. Восстановление при сбоях и обеспечение непрерывности деятельности

Оператор гарантирует, что в случае сбоя, включая компрометацию личных ключей РУЦ, действия будут возобновлены после устранения сбоя, в минимально короткое время.

Оператором разработан план восстановительных работ при сбоях и обеспечении непрерывности деятельности.

Данные РУЦ, необходимые для продолжения его деятельности, подвергаются резервному копированию и хранятся в двух различных безопасных местах, пригодных для того, чтобы РУЦ мог оперативно возобновить деятельность в случае аварии или сбоя.

В случае компрометации личного ключа РУЦ Оператор в установленном порядке информирует об этом ОАЦ, всех подписчиков и доверяющие стороны, с которыми заключены договоры или другие формы соглашений, а также объявляет о том, что все сертификаты и СОС, изданные с использованием данного ключа РУЦ, более не являются действительными.

3.3.9. Прекращение функционирования РУЦ

Оператор гарантирует, что потенциальные угрозы для подписчиков и доверяющих сторон будут сведены к минимуму в результате прекращения предоставления услуг РУЦ, а также что информация о сертификатах будет сохранена для предоставления в суд, в случае необходимости.

В случае прекращения функционирования РУЦ:

информирует ОАЦ, всех подписчиков и доверяющие стороны, с которыми он заключил гражданско-правовые договоры или другие формы соглашений;

осуществляет необходимые процедуры по передаче обязанностей для хранения регистрационной информации и записей архивов, включая информацию о статусе отзыва на соответствующий период, оговоренный с подписчиками и доверяющими сторонами;

уничтожает под контролем комиссии свои личные ключи без возможности их восстановления;

гарантирует, что потенциальные угрозы для подписчиков и доверяющих сторон будут сведены к минимуму в результате прекращения предоставления услуг РУЦ, а информация о сертификатах будет сохранена для представления по требованию уполномоченных государственных органов и судов в порядке, установленном законодательными актами.

РУЦ обеспечивает возможность покрывать затраты по выполнению минимальных требований в случае его банкротства или отсутствия возможности оплатить все затраты самостоятельно по другим причинам, насколько это возможно в рамках действующего законодательства о банкротстве.

3.3.10. Соответствие требованиям законодательства

РУЦ поддерживает в ГосСУОК технологию ЭЦП в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи».

РУЦ защищает информацию, распространение и (или) предоставление которой ограничено, не отнесенную к государственным секретам, в соответствии с требованиями, установленными Законом Республики Беларусь «Об информации, информатизации и защите информации», Положением о технической и криптографической защите информации в Республике Беларусь, утвержденным Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 и другими действующими нормативными правовыми актами в области защиты информации.

3.3.11. Сохранение информации, касающейся сертификатов

РУЦ гарантирует, что вся информация, относящаяся к сертификатам (регистрационная, об издании и отзыве) сохраняется на установленный срок, в частности, с целью ее предоставления в суд по искам к электронным документам, на следующие сроки:

в РУЦ – в течение времени действия сертификата подписчика;

в государственном архиве – в соответствии с законодательством Республики Беларусь.

РУЦ поддерживает конфиденциальность и целостность текущих и архивированных записей, касающихся сертификатов.

РУЦ предоставляет доступ к записям, касающимся сертификатов, в целях представления их в суд. Потребители и субъекты могут получить доступ к регистрационной и другой информации в соответствии с требованиями, установленными в Законе Республики Беларусь «Об информации, информатизации и защите информации».

РУЦ обеспечивает поддержку точного времени событий в информационной системе РУЦ, системе управления ключами ЭЦП и сертификатами.

РУЦ обеспечивает хранение записей, касающихся сертификатов, в течение периода времени, необходимого для подтверждения ЭЦП в электронных документах.

РУЦ обеспечивает регистрацию событий таким образом, чтобы они не были несанкционированно удалены (кроме переноса на долгосрочные средства хранения информации) в течение периода времени, когда они хранятся.

События и данные, которые должны регистрироваться, документируются Оператором.

Оператор регистрирует все события, связанные с регистрацией подписчиков, запросы на издание, обновление и отзыв сертификатов.

РУЦ (РЦ) сохраняет всю регистрационную информацию, включая:

– номер документа заявителя, удостоверяющего его личность в соответствии с законодательством Республики Беларусь, дату выдачи данного документа, наименование органа, выдавшего его, идентификационный номер;

– копии документов, необходимых для оказания услуг.

Оператор обеспечивает конфиденциальность, целостность и подлинность регистрационной информации.

РУЦ (РЦ) регистрирует все события, связанные со сроком действия личных ключей подписи РУЦ, со сроком действия изданных сертификатов, отзывом сертификатов.

3.4. Организационные положения

РУЦ обеспечивает оказание услуг любым организациям и физическим лицам, заинтересованным в получении услуг РУЦ и обратившимся в РУЦ или РЦ.

Оператор может привлекать сторонние организации для оказания услуг РЦ конечным пользователям РУЦ (далее - пользователи). Услуги РЦ, оказываемые сторонними организациями, иными третьими сторонами в отношении РУЦ, должны выполняться (оказываться) на основании соответствующих гражданских договоров, заключаемых Оператором с лицами или организациями, привлекаемыми для оказания таких услуг.

Применение соответствующей ППС и настоящего Регламента основано на ее добровольном признании подписчиком. Признание ППС является необходимым условием для получения услуг РУЦ. Ответственность РУЦ предусматривается в договоре, заключаемом Оператором с подписчиком, которому оказываются соответствующие услуги.

С подписчиком РУЦ может быть заключен публичный договор, который размещается на Интернет-сайте Оператора. Условия публичного договора являются общими для всех подписчиков РУЦ. Оператор оставляет за собой право не рассматривать и не обсуждать предложения подписчиков РУЦ по изменению и (или) дополнению условий публичного договора. Факт принятия (акцепта) подписчиком РУЦ условий публичного договора выражается в оплате подписчиком РУЦ услуги РУЦ. Публичный договор при условии соблюдения порядка его оплаты, считается заключенным в простой письменной форме. Публичный договор является действительным в той редакции и на тех условиях, которые существовали на момент оплаты услуг РУЦ.

В РУЦ рассмотрение обращений и жалоб, поступающих от подписчиков, а также порядок разрешения споров, возникающих в связи с оказанием услуг проводится в соответствии с постановлением Совета Министров Республики Беларусь от 16 марта 2005 г. № 285 «О некоторых вопросах организации работы с книгой замечаний и предложений и внесении изменений и дополнений в некоторые постановления Совета министров Республики Беларусь».

Деятельность структурных подразделений Оператора, выполняющих процедуры оказания услуг по распространению открытых ключей, не должна зависеть от действий и решений сторонних организаций, в том числе в принятии решений о предоставлении и приостановлении услуг, порядке их оказания.

Структурные подразделения Оператора, выполняющие процедуры оказания услуг по распространению открытых ключей, должны иметь штатную структуру, позволяющую гарантировать объективность и независимость принимаемых решений и осуществляемых действий.

Оператор обладает необходимыми материальными и финансовыми возможностями, позволяющими ему надлежащим образом обеспечивать выполнение настоящего Регламента и соответствующей ППС.