Утвержден директором
государственного
предприятия «НЦЭУ»
22.04.2020

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

Минск
2020

СОДЕРЖАНИЕ

1. Введение в регламент деятельности

1.1. Общие положения

Настоящий регламент деятельности республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – регламент) является документом, устанавливающим основные правила деятельности республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – республиканский удостоверяющий центр), и разработан в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров».

Для целей регламента термины и определения используются в значениях, определенных Законом Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи», СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей», СТБ 34.101.48-2012, СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов», СТБ 34.101.69-2014 «Информационные технологии и безопасность. Криптология. Термины и определения».

В соответствии с пунктом 5 Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» функции оператора республиканского удостоверяющего центра осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее — оператор).

Оператор осуществляет оказание услуг республиканского удостоверяющего центра на договорной основе.

Юридический адрес оператора:
ул. Раковская, 14
220004, г. Минск, Республика Беларусь.
УНП 191700161, ОКПО 380325925000.

Контактная информация:
телефон: 8 (017) 311 30 00;
факс: 8 (017) 311 30 06;
e-mail: info@nces.by;
интернет-сайт: nces.by.

Основные функции республиканского удостоверяющего центра определены в Положении о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь,

утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118.

1.2. Пользователи регламента

Сертификаты открытых ключей проверки электронной цифровой подписи (далее – сертификаты) и атрибутные сертификаты, изданные в соответствии с регламентом, могут быть использованы для целей, определенных соответствующей политикой применения сертификатов, политикой применения атрибутных сертификатов.

2. Требования к участникам инфраструктуры открытых ключей

2.1. Требования к республиканскому удостоверяющему центру

Республиканский удостоверяющий центр обязан выполнять все требования, установленные соответствующей политикой применения сертификатов, политикой применения атрибутных сертификатов, а также регламента, положения которого не противоречат указанным политикам.

2.2. Требования к регистрационному центру

Регистрационный центр осуществляет свою деятельность в соответствии с регламентом работы, согласованным с оператором.

Регистрационный центр обязан выполнять все требования, установленные соответствующей политикой применения сертификатов, политикой применения атрибутных сертификатов, а также регламента, положения которого не противоречат указанным политикам.

Регистрационный центр должен быть аккредитован в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь в соответствии с требованиями Инструкции о порядке проведения аккредитации поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и осуществления контроля за соблюдением условий аккредитации, утвержденной приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.11.2013 № 89.

Основные функции регистрационного центра определены в Положении о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118.

Регистрационный центр несет ответственность за проверку информации, вносимой в сертификаты и атрибутные сертификаты.

2.3. Требования к подписчикам

Подписчики обязаны:

гарантировать, что вся информация, предоставляемая для издания сертификатов и (или) атрибутных сертификатов, является полной и точной;

использовать личный и открытый ключи только для выработки и проверки электронной цифровой подписи, а также в соответствии с ограничениями, о которых оператор уведомляет подписчика;

хранить в тайне личный ключ;

обеспечивать защиту личного ключа от случайного уничтожения или от 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 этого открытого ключа истек.

2.4. Требования к доверяющей стороне

Доверяющие стороны могут запрашивать у оператора сертификаты и атрибутные сертификаты любого подписчика и использовать их для проверки электронной цифровой подписи электронного документа.

Перед установлением доверия к электронному документу доверяющая сторона обязана:

убедиться в действительности сертификата и атрибутного сертификата, включая их проверку на отзыв или истечение срока действия;

удостовериться, что в атрибутном сертификате содержится информация о полномочиях физического лица.

2.5. Требования к центру атрибутных сертификатов

Центр атрибутных сертификатов на основании сертификатов физических лиц, работающих в государственных органах и других организациях, а также иных физических лиц издает атрибутные сертификаты в соответствии с политикой применения атрибутных сертификатов.

В атрибутных сертификатах содержится информация о полномочиях таких физических лиц.

Функции центра атрибутных сертификатов осуществляет республиканский удостоверяющий центр.

3. Требования к республиканскому удостоверяющему центру

3.1. Требования по управлению ключами

3.1.1. Выработка личного ключа республиканского удостоверяющего центра, центра атрибутных сертификатов

Выработка личных ключей и открытых ключей республиканского удостоверяющего центра и центра атрибутных сертификатов 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, имеющего сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

Порядок выработки личного ключа подписи и формирование запроса к корневому удостоверяющему центру на издание сертификата республиканского удостоверяющего центра определен в организационно-распорядительных документах оператора.

Порядок выработки личного ключа и открытого ключа центра атрибутных сертификатов определяется в организационно-распорядительных документах оператора.

Срок действия сертификата республиканского удостоверяющего центра – 15 лет.

Срок действия сертификата центра атрибутных сертификатов – 10 лет.

До истечения срока действия личного ключа подписи республиканского удостоверяющего центра оператор вырабатывает новую пару ключей для подписи издаваемых сертификатов и принимает все необходимые меры для того, чтобы избежать нарушения деятельности любого участника, доверяющего сертификату республиканского удостоверяющего центра. Новые ключи республиканского удостоверяющего центра создаются и распространяются в соответствии с регламентом деятельности республиканского удостоверяющего центра.

До истечения срока действия личного ключа подписи центра атрибутных сертификатов оператор вырабатывает новую пару ключей для подписи издаваемых атрибутных сертификатов и принимает все необходимые меры для того, чтобы избежать нарушения деятельности любого участника, доверяющего сертификату центра атрибутных сертификатов. Новые ключи центра атрибутных сертификатов создаются и распространяются в соответствии с регламентом.

3.1.2. Хранение, резервное копирование и восстановление личного ключа республиканского удостоверяющего центра, центра атрибутных сертификатов

Личные ключи республиканского удостоверяющего центра и центра атрибутных сертификатов хранятся в тайне и используются только в сертифицированном программно-аппаратном средстве электронной цифровой подписи.

Средства контроля доступа к программно-аппаратному средству электронной цифровой подписи, в котором хранятся личные ключи республиканского удостоверяющего центра и центра атрибутных сертификатов, гарантируют отсутствие несанкционированного доступа к ним.

Работники оператора осуществляют резервное копирование личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов. Резервные копии личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов хранятся в зашифрованном виде.

К ключам шифрования резервных копий личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов 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 личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов, их восстановление осуществляется в присутствии как минимум двух подготовленных и доверенных работников оператора в отдельном помещении на программно-аппаратном средстве электронной цифровой подписи под контролем комиссии (владельцы частичных секретов резервной копии личных ключей различны).

Безопасность резервных копий личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов обеспечивается на таком же или более высоком уровне, как и для постоянно используемых личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов.

3.1.3. Распространение открытых ключей республиканского удостоверяющего центра, центра атрибутных сертификатов

Республиканский удостоверяющий центр распространяет свой открытый ключ в виде сертификата, подписанного личным ключом корневого удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Центр атрибутных сертификатов распространяет свой открытый ключ в виде сертификата, подписанного личным ключом республиканского удостоверяющего центра.

Сертификаты республиканского удостоверяющего центра и центра атрибутных сертификатов размещаются на интернет-сайте оператора.

Доверяющие стороны должны проводить проверку подлинности и целостности открытых ключей республиканского удостоверяющего центра и центра атрибутных сертификатов при их получении.

3.1.4. Депонирование личного ключа республиканского удостоверяющего центра, центра атрибутных сертификатов

Республиканский удостоверяющий центр и центр атрибутных сертификатов не осуществляют депонирование личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов, несмотря на то, что они осуществляют их резервное копирование.

3.1.5. Использование личного ключа республиканского удостоверяющего центра, центра атрибутных сертификатов

Республиканский удостоверяющий центр использует свой личный ключ только для издания сертификатов, списков отозванных сертификатов и предоставления информации о статусе сертификатов, определенных в соответствующей политике применения сертификатов.

Центр атрибутных сертификатов использует свой личный ключ только для издания атрибутных сертификатов, списков отозванных атрибутных сертификатов и предоставления информации о статусе атрибутных сертификатов, определенных в политике применения атрибутных сертификатов.

3.1.6. Окончание срока действия личного ключа республиканского удостоверяющего центра, центра атрибутных сертификатов

Личные ключи республиканского удостоверяющего центра и центра атрибутных сертификатов не используются по окончании срока их действия.

Уничтожение копий личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов без возможности восстановления всех копий личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов, в том числе и резервных, осуществляется после окончания срока их действия в порядке, определенном в организационно-распорядительных документах оператора.

3.1.7. Управление средством электронной цифровой подписи, используемым для издания сертификатов, атрибутных сертификатов

В республиканском удостоверяющем центре и центре атрибутных сертификатов для издания сертификатов и атрибутных сертификатов, списков отозванных сертификатов и списков отозванных атрибутных сертификатов используется программно-аппаратное средство электронной цифровой подписи, имеющее сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

Оператор обеспечивает безопасность программно-аппаратного средства электронной цифровой подписи в течение всего срока его применения для издания сертификатов и атрибутных сертификатов, списков отозванных сертификатов и списков отозванных атрибутных сертификатов.

Оператор гарантирует, что:

программно-аппаратное средство электронной цифровой подписи не было повреждено во время поставки;

программно-аппаратное средство электронной цифровой подписи не было скомпрометировано во время хранения;

установка, активация, резервное копирование и восстановление личных ключей республиканского удостоверяющего центра и центра атрибутных сертификатов в программно-аппаратном средстве электронной цифровой подписи проводится под контролем как минимум двух доверенных работников оператора и владельцев порогового числа частичных секретов, участвующих в восстановлении под контролем комиссии;

программно-аппаратное средство электронной цифровой подписи функционирует правильно;

личные ключи республиканского удостоверяющего центра и центра атрибутных сертификатов, хранимые в программно-аппаратном средстве электронной цифровой подписи, уничтожаются при изъятии данного средства из обращения.

3.2. Требования по управлению сертификатами, атрибутными сертификатами

3.2.1. Регистрация подписчика

Регистрация подписчиков осуществляется регистрационными центрами.

О нормах и правилах, касающихся использования сертификата (атрибутного сертификата) подписчик информируется республиканским удостоверяющим центром в соответствии с п.п. 3.2.4 регламента.

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

В отношении подписчиков (физических лиц) – резидентов Республики Беларусь регистрируется вся информация, однозначно идентифицирующая физическое лицо, а также информация о документе, удостоверяющем личность в соответствии с законодательством Республики Беларусь (серия и номер документа, дата выдачи и наименование органа, выдавшего такой документ), содержащаяся в самом документе, удостоверяющем личность, или в государственной информационной системе (ресурсе).

В отношении подписчиков (физических лиц) – нерезидентов Республики Беларусь регистрируются данные, имеющиеся в представленном документе, удостоверяющем личность.

Информация о полномочиях, предоставленных физическому лицу (представителю организации или другого физического лица), проверяется на основании документов, подтверждающих такие полномочия.

Проверка подлинности информации об организации (обособленном подразделении юридического лица (филиала), индивидуального предпринимателя, нотариуса, адвоката), проводится на основании документов и сведений, выданных регистрирующими органами (в части полного наименования и правового статуса, иной регистрационной информации).

Перечень документов, представляемых подписчиками, а также уточненный перечень регистрируемых данных определяется в порядке оказания услуг республиканского удостоверяющего центра и иных организационно-распорядительных документах оператора.

При регистрации подписчика процесс формирования запроса на издание сертификата гарантирует, что физическое лицо (в том числе, индивидуальный предприниматель, нотариус, адвокат) или организация (в том числе, обособленное подразделение юридического лица (филиал)) владеют 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».

Оператор обеспечивает конфиденциальность и целостность регистрационных данных, передаваемых при обмене с подписчиком, владельцем сертификата или между компонентами инфраструктуры оператора, задействованными в процессах оказания услуг республиканского удостоверяющего центра.

Подлинность и целостность регистрационных данных в электронном виде заверяется с помощью действительных сертификатов регистрационных центров.

3.2.2. Возобновление действия сертификата, атрибутного сертификата и обновление данных

Республиканский удостоверяющий центр 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.

Центр атрибутных сертификатов осуществляет возобновление действия атрибутного сертификата путем издания нового атрибутного сертификата, сохранив без изменения информацию, содержащуюся в атрибутном сертификате (кроме срока действия атрибутного сертификата), предварительно убедившись, что на момент обращения она является действительной.

Обновление данных сертификата (атрибутного сертификата) осуществляется путем отзыва действующего сертификата (атрибутного сертификата) и издания нового сертификата (атрибутного сертификата) с внесением в сертификат (атрибутный сертификат) обновленной информации (за исключением регистрационного номера организации).

Новый атрибутный сертификат издается в пределах срока действия сертификата, в дополнение к которому он издается.

Последовательность действий регистрационного центра, подписчика и перечень представляемых подписчиком документов указаны в организационно-распорядительных документах оператора.

3.2.3. Издание сертификата, атрибутного сертификата

Республиканский удостоверяющий центр издает сертификаты способом, обеспечивающим сохранение их подлинности и целостности

Перед изданием сертификата осуществляется проверка личности физического лица (данных о государственной регистрации организации), а также полнота и точность представленных подписчиком данных. При этом личность физического лица проверяется на основании:

документа, удостоверяющего личность (при оказании услуг республиканского удостоверяющего центра в регистрационном центре);

сведений, содержащихся в действующем сертификате (при оказании услуг республиканского удостоверяющего центра через Единый портал электронных услуг). Информация, которая при этом подтверждается, - это фамилия, имя, отчество (при наличии) и идентификационный номер).

Центр атрибутных сертификатов издает атрибутные сертификаты способом, обеспечивающим сохранение их подлинности и целостности

Содержание основных полей издаваемых сертификатов и атрибутных сертификатов устанавливаются в соответствующих политиках применения сертификатов и политике применения атрибутных сертификатов.

Формат сертификата соответствует СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».

Республиканский удостоверяющий центр гарантирует уникальность идентификационного номера сертификата.

Центр атрибутных сертификатов гарантирует уникальность идентификационного номера атрибутного сертификата.

Атрибутный сертификат издается в пределах срока действия сертификата, к которому он издается.

3.2.4. Распространение организационно-распорядительных документов

Оператор гарантирует, что необходимые организационно-распорядительные документы являются доступными для подписчиков и доверяющих сторон.

Оператор предоставляет доступ подписчикам и доверяющим сторонам к следующим организационно-распорядительным документам:

копия аттестата об аккредитации республиканского удостоверяющего центра в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь;

регламент;

политики применения сертификатов, политика применения атрибутных сертификатов;

порядок оказания услуг республиканского удостоверяющего центра;

адреса и контактные данные республиканского удостоверяющего центра и регистрационных центров;

перечень информационных систем, использующих сертификаты, изданные республиканским удостоверяющим центром;

публичные договоры на оказание услуг республиканского удостоверяющего центра;

перечень документов, необходимых для оказания услуг республиканского удостоверяющего центра;

прейскурант тарифов на услуги республиканского удостоверяющего центра;

иные документы, установленные в соответствующих политиках применения сертификатов, политике применения атрибутных сертификатов, технических нормативных правовых актах.

Оператор предоставляет организационно-распорядительные документы с использованием долговечных носителей информации (т.е. сохраняющих целостность в течение длительного времени), в том числе в электронном виде, на государственном(ых) языке(ах) Республики Беларусь.

3.2.5. Распространение сертификатов, атрибутных сертификатов

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

Атрибутный сертификат становится действительным с даты начала действия, указанного в атрибутном сертификате.

Изданные сертификаты и атрибутные сертификате помещаются в хранилище республиканского удостоверяющего центра и передаются подписчику в соответствии с порядком оказания услуг республиканского удостоверяющего центра.

Информация о назначении сертификата содержится в самом сертификате.

Описание основных полей форматов издаваемых сертификатов и атрибутных сертификатов описаны в приложениях к соответствующим политикам применения сертификатов и политике применения атрибутных сертификатов.

Данная информация 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 информация будет недоступна только в течение времени, установленного в соответствующей политике применения сертификатов, политике применения атрибутных сертификатов.

3.2.6. Отзыв сертификата, атрибутного сертификата

Отзыв сертификата влечет за собой отзыв атрибутного сертификата, связанного с указанным сертификатом.

Республиканский удостоверяющий центр гарантирует, что сертификат и (или) атрибутный сертификат отзывается на основании запроса в сроки и в порядке, установленные в соответствующей политике применения сертификатов и (или) политике применения атрибутных сертификатов.

Республиканский удостоверяющий центр идентифицирует и проверяет запросы, связанные с отзывом сертификатов и атрибутных сертификатов, на предмет их получения из достоверных источников.

Если сертификат и (или) атрибутный сертификат отозван, он никогда не должен использоваться в дальнейшем.

Услуги республиканского удостоверяющего центра по управлению отзывом доступны в течение рабочего времени регистраторов. 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 политике применения сертификатов или политике применения атрибутных сертификатов.

3.2.7. Предоставление информации о статусе сертификата, атрибутного сертификата

При распространении республиканским удостоверяющим центром (центром атрибутных сертификатов) информации о статусе сертификата (атрибутного сертификата) посредством издания списка отозванных сертификатов (списка отозванных атрибутных сертификатов) такие списки издаются и публикуются в реальном времени, а также:

каждый список отозванных сертификатов и список отозванных атрибутных сертификатов издаются не реже одного раза в месяц и содержат информацию о времени издания следующих списка отозванных сертификатов и соответственно списка отозванных атрибутных сертификатов;

новый список отозванных сертификатов и список отозванных атрибутных сертификатов могут быть опубликованы перед установленным временем издания следующих списка отозванных сертификатов и соответственно списка отозванных атрибутных сертификатов;

список отозванных сертификатов и список отозванных атрибутных сертификатов подписываются личным ключом республиканского удостоверяющего центра и соответственно центра атрибутных сертификатов;

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

Услуги республиканского удостоверяющего центра по получению статуса сертификата и атрибутного сертификата доступны 24 часа в сутки 365 дней в году посредством размещения списка отозванных сертификатов и списка отозванных атрибутных сертификатов на официальном интернет-сайте оператора, а также через службу предоставления информации о действительности сертификатов и атрибутных сертификатов в соответствии с СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)».

Порядок получения доступа к OCSP-серверу и его использования для получения информации о статусе сертификата или атрибутного сертификата, определяется оператором в организационно-распорядительных документах.

В случае отказа системы, сервисов или при наличии других факторов, не зависящих от оператора, оператор принимает все необходимые меры, чтобы гарантировать, что данные услуги будут недоступны только в течение времени, установленного в соответствующей политике применения сертификатов или политике применения атрибутных сертификатов.

3.3. Управление деятельностью республиканского удостоверяющего центра

3.3.1. Управление безопасностью

Система защиты информации автоматизированной информационной системы республиканского удостоверяющего центра аттестована в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

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

Требования к системе защиты информации 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 системе защиты информации или автоматизированной информационной системы республиканского удостоверяющего центра). Работы по оценке рисков проводятся в сроки и порядке, определенном в Политике информационной безопасности республиканского удостоверяющего центра.

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

3.3.2. Классификация и управление активами

Все критические активы республиканского удостоверяющего центра, требования и меры по их защите определены в задании по безопасности автоматизированной информационной системы республиканского удостоверяющего центра, на предмет соответствия которого проведена аттестация системы защиты информации автоматизированной информационной системы республиканского удостоверяющего центра в реальных условиях эксплуатации.

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

3.3.3. Вопросы безопасности, связанные с персоналом

На должности привлекаются работники оператора, которые обладают необходимой квалификацией, опытом и прошли проверку на соответствие кадровой политике оператора, что подтверждается внутренними локальными

правовыми актами, регламентирующими деятельность республиканского удостоверяющего центра.

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 республиканского удостоверяющего центра.

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 республиканском удостоверяющем центре поддерживаются следующие роли работников с соответствующими обязанностями:

администратор информационной безопасности: отвечает за администрирование системы защиты информации автоматизированной информационной системы республиканского удостоверяющего центра; осуществляет контроль целостности и подлинности текущих и архивных системных журналов событий и инцидентов безопасности автоматизированной информационной системы республиканского удостоверяющего центра, проведение аудита безопасности системы защиты информации автоматизированной информационной системы республиканского удостоверяющего центра;

системный администратор: отвечает за установку, конфигурирование и обслуживание автоматизированной информационной системы республиканского удостоверяющего центра, используемой для регистрации, издания и отзыва сертификатов (атрибутных сертификатов); за повседневное обслуживание автоматизированной информационной системы республиканского удостоверяющего центра; осуществляет резервное копирование и восстановление автоматизированной информационной системы республиканского удостоверяющего центра;

администратор баз данных: отвечает за управление, архивирование, резервное копирование и восстановление баз данных автоматизированной информационной системы республиканского удостоверяющего центра.

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 Оперативно-аналитическом центре при Президенте Республики Беларусь.

3.3.4. Физическая защита и защита от воздействий окружающей среды

Оператор обеспечивает физический доступ к оборудованию, используемому для издания 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 республиканском удостоверяющем центре. Безопасность серверного центра республиканского удостоверяющего центра проанализирована при проведении аттестации системы защиты информации автоматизированной информационной системы республиканского удостоверяющего центра и аккредитации республиканского удостоверяющего центра в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

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

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

В организационно-распорядительных документах оператора, разработанных в рамках реализации мероприятий по обеспечению информационной безопасности, описаны средства защиты всего оборудования республиканского удостоверяющего центра, 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, техническое обслуживание оборудования, системы обнаружения физического вторжения и т.д.

3.3.5. Управление операционной деятельностью

Автоматизированная информационная система республиканского удостоверяющего центра и информация, обрабатываемая в автоматизированной

информационной системе республиканского удостоверяющего центра, защищены от вирусов и не доверенного программного обеспечения.

В автоматизированной информационной системе республиканского удостоверяющего центра протоколируются все сбои и инциденты безопасности, а также СЗИ применяются меры быстрого реагирования на данные события.

В задании по безопасности автоматизированной информационной системы республиканского удостоверяющего центра определены процедуры, влияющие на предоставление услуг по распространению открытых ключей, политика управления носителями информации, используемыми в рамках деятельности республиканского удостоверяющего центра для защиты их от повреждения, хищения и несанкционированного доступа к ним, а также политика по контролю журналов аудита автоматизированной информационной системы республиканского удостоверяющего центра 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 системы защиты информации автоматизированной информационной системы республиканского удостоверяющего центра, а также на инциденты в области информационной и системной безопасности и ограничению влияния при нарушении безопасности.

В республиканском удостоверяющем центре процессы проверки соответствия требованиям сохранности информации о сертификатах и атрибутных сертификатах начинаются при запуске автоматизированной информационной системы республиканского удостоверяющего центра и заканчиваются при ее остановке.

В республиканском удостоверяющем центре операции по обеспечению безопасности отделены от любых других операций.

В политике информационной безопасности и должностных инструкциях работников определены обязанности по обеспечению безопасности республиканского удостоверяющего центра, 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 проверку исполнения, управление носителями информации и их безопасность, обмен данными и программным обеспечением.

3.3.6. Управление системным доступом

Автоматизированная информационная система республиканского удостоверяющего центра представляет собой информационную систему, на которой обрабатывается информация, охраняемая в соответствии с законодательством Республики Беларусь. Технические средства автоматизированной информационной системы республиканского удостоверяющего центра размещены в одной контролируемой зоне, и обработка защищаемой информации осуществляется в пределах области действия комплекса средств безопасности объекта.

В системе защиты информации автоматизированной информационной системы республиканского удостоверяющего центра применяются сертифицированные средства криптографической защиты информации для обеспечения конфиденциальности, контроля целостности (неизменности) и подлинности информации, распространение и (или) предоставление которой ограничено.

В автоматизированной информационной системе республиканского удостоверяющего центра управление доступом пользователей (включая регистраторов регистрационных центров, 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 республиканского удостоверяющего центра.

В республиканском удостоверяющем центре ответственные работники перед использованием оборудования и программного обеспечения, связанного с управлением сертификатами и списками отозванных сертификатов, проходят процедуру двухфакторной идентификации и аутентификации.

Действия работников контролируются путем сохранения записей событий.

В республиканском удостоверяющем центре 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 автоматизированной информационной системе республиканского удостоверяющего центра локальные сетевые компоненты (например, маршрутизаторы) располагаются в физически безопасном окружении и их конфигурация периодически проверяется на соответствие требованиям, установленным в политике информационной безопасности республиканского удостоверяющего центра.

В помещениях, в которых размещены активы автоматизированной информационной системы республиканского удостоверяющего центра, 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 автоматизированной информационной системе республиканского удостоверяющего центра используются безопасные доверенные информационные системы и продукты, которые защищены от модификации, и сертифицированные средства управления криптографическими ключами, сертификатов и атрибутных сертификатов, списков отозванных сертификатов и списков отозванных атрибутных сертификатов.

Анализ требований безопасности проводится на всех этапах разработки и эксплуатации информационных систем и продуктов, используемых в автоматизированной информационной системе республиканского удостоверяющего центра 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 республиканского удостоверяющего центра, действия будут возобновлены после устранения сбоя в минимально короткое время.

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

Данные республиканского удостоверяющего центра, необходимые для продолжения его деятельности, подвергаются резервному копированию для того, чтобы республиканский удостоверяющий центр мог оперативно возобновить деятельность в случае аварии или сбоя.

В случае компрометации личного ключа республиканского удостоверяющего центра оператор в установленном порядке информирует об этом Оперативно-аналитический центр при Президенте Республики Беларусь, всех подписчиков и доверяющие стороны, с которыми заключены договоры или другие формы соглашений, а также объявляет о том, что все сертификаты и списки отозванных сертификатов, изданные с использованием данного ключа республиканского удостоверяющего центра, более не являются действительными.

3.3.9. Прекращение функционирования республиканского удостоверяющего центра

Оператор гарантирует, что потенциальные угрозы для подписчиков и доверяющих сторон будут сведены к минимуму в результате прекращения предоставления услуг республиканского удостоверяющего центра, а также, что

информация о сертификатах будет сохранена для предоставления в суд, в случае необходимости.

В случае прекращения функционирования республиканский удостоверяющий центр:

информирует Оперативно-аналитический центр при Президенте Республики Беларусь, 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 республиканского удостоверяющего центра, а информация о сертификатах будет сохранена для представления по требованию уполномоченных государственных органов и судов в порядке, установленном законодательными актами.

Республиканский удостоверяющий центр 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

Республиканский удостоверяющий центр поддерживает в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь технологию электронной цифровой подписи в соответствии с Законом Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

Республиканский удостоверяющий центр защищает информацию, распространение и (или) предоставление которой ограничено, не отнесенную к государственным секретам, в соответствии с требованиями, установленными Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», и действующими нормативными правовыми актами в области защиты информации.

3.3.11. Сохранение информации, касающейся сертификатов, атрибутных сертификатов

Республиканский удостоверяющий центр гарантирует, что вся информация, относящаяся к сертификатам и атрибутным 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 республиканском удостоверяющем центре – в течение времени действия сертификата подписчика;

в государственном архиве – в соответствии с законодательством Республики Беларусь.

Республиканский удостоверяющий центр поддерживает конфиденциальность и целостность текущих и архивированных записей, касающихся сертификатов и атрибутных сертификатов.

Республиканский удостоверяющий центр предоставляет доступ к записям, касающимся сертификатов и атрибутных сертификатов, в целях представления их в суд. Государственные органы и организации, а также физические лица (в том числе индивидуальные предприниматели) могут получить доступ к регистрационной и другой информации в соответствии с требованиями, установленными в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» и иными нормативными правовыми актами.

Республиканский удостоверяющий центр обеспечивает поддержку точного времени событий в автоматизированной информационной системе республиканского удостоверяющего центра.

Республиканский удостоверяющий центр обеспечивает хранение записей, касающихся сертификатов и атрибутных сертификатов, в течение периода времени, необходимого для подтверждения электронной цифровой подписи в электронных документах.

Республиканский удостоверяющий центр 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 и атрибутных сертификатов.

Республиканский удостоверяющий центр сохраняет всю регистрационную информацию.

Оператор обеспечивает конфиденциальность и целостность и подлинность регистрационной информации.

Республиканский удостоверяющий центр регистрирует все события, связанные со сроком действия личных ключей подписи республиканского удостоверяющего центра, со сроком действия изданных сертификатов (атрибутных сертификатов), отзывом сертификатов (атрибутных сертификатов).

3.4. Организационные положения

Республиканский удостоверяющий центр обеспечивает оказание услуг любым физическим лицам, индивидуальным предпринимателям и организациям, обособленным подразделениям юридических лиц (филиалам), нотариусам и адвокатам, заинтересованным в получении услуг республиканского удостоверяющего центра и обратившимся в республиканский удостоверяющий центр или регистрационный центр.

Оператор может привлекать сторонние организации для оказания услуг подписчикам республиканского удостоверяющего центра. Услуги, оказываемые сторонними организациями, иными третьими сторонами, выполняются (оказываются) на основании соответствующих гражданских договоров, заключаемых оператором с лицами или организациями, привлекаемыми для оказания таких услуг.

Применение соответствующей политики применения сертификатов и (или) политики применения атрибутных сертификатов, а также регламента деятельности республиканского удостоверяющего центра основано на их добровольном признании подписчиком. Признание является необходимым условием для получения услуг республиканского удостоверяющего центра.

Ответственность республиканского удостоверяющего центра предусматривается в договоре, заключаемом оператором с подписчиком, которому оказываются услуги республиканского удостоверяющего центра.

С подписчиком может быть заключен публичный договор, который размещается на официальном интернет-сайте оператора. Условия публичного договора являются общими для всех подписчиков республиканского удостоверяющего центра. Оператор оставляет за собой право не рассматривать и не обсуждать предложения подписчиков по изменению и (или) дополнению условий публичного договора. Факт принятия (акцепта) подписчиком республиканского удостоверяющего центра условий публичного договора выражается в оплате подписчиком услуги республиканского удостоверяющего центра. 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 республиканского удостоверяющего центра.

В республиканском удостоверяющем центре рассмотрение обращений и жалоб, поступающих от подписчиков, а также порядок разрешения споров, возникающих в связи с оказанием услуг, проводится в соответствии с Законом Республики Беларусь от 18.07.2011 № 300-З «Об обращениях граждан и юридических лиц».

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 регламента республиканского удостоверяющего центра и соответствующих политик применения сертификатов и политики применения атрибутных сертификатов.

Регламент вступает в силу с 23.04.2020.