ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
8 февраля 2019 г. № 45

О дополнительных мерах по реализации Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»

На основании части третьей статьи 26, части четвертой статьи 26^1, частей пятой и седьмой статьи 29 Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» ПРИКАЗЫВАЮ:

1. Установить, что:

1.1. при обращении организации или физического лица, в том числе индивидуального предпринимателя (далее – заявитель), к поставщику услуг за изданием сертификата открытого ключа проверки электронной цифровой подписи (далее – сертификат), личный ключ электронной цифровой подписи которого заявитель выработал самостоятельно (без использования технических средств регистрационного центра) с помощью сертифицированного средства электронной цифровой подписи, заявитель представляет поставщику услуг данные в соответствии с политикой применения сертификатов поставщика услуг и открытый ключ проверки электронной цифровой подписи, которые необходимо включить в сертификат.

Для подтверждения владения заявителем личным ключом электронной цифровой подписи поставщик услуг:

проверяет полноту и точность представленных данных заявителя, в том числе личность физического лица, данные о государственной регистрации организации, согласно политике применения сертификатов поставщика услуг;

на основании представленных данных формирует запрос на получение сертификата в соответствии с требованиями СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата» в электронном виде.

Заявитель с использованием сертифицированного средства электронной цифровой подписи подписывает сформированный запрос на получение сертификата личным ключом электронной цифровой подписи, открытый ключ проверки электронной цифровой подписи которого включен в этот запрос.

Поставщик услуг с использованием сертифицированного средства электронной цифровой подписи проверяет подписанный запрос на получение сертификата в соответствии с СТБ 34.101.17-2012.

В случае если подлинность и целостность запроса на получение сертификата подтверждаются, считается, что заявитель владеет указанным личным ключом электронной цифровой подписи;

1.2. при обращении к поставщику услуг за изданием атрибутного сертификата заявитель представляет информацию о (об):

сертификате, с которым будет связан атрибутный сертификат, физическом лице, являющемся владельцем этого сертификата и которому от имени заявителя предоставлены полномочия на подписание определенных видов электронных документов, а также об иных полномочиях (далее – полномочия), заявителе, предоставившем полномочия физическому лицу;

полномочиях, предоставленных физическому лицу.

Информация, указанная в части первой настоящего подпункта, может быть представлена в виде электронного документа, подписанного электронной цифровой подписью заявителя.

Для издания атрибутного сертификата поставщик услуг обязан:

проверить связь физического лица, которому предоставляются полномочия, с заявителем, а также эти полномочия;

установить принадлежность сертификата физическому лицу, которому предоставляются полномочия, а также убедиться в действительности этого сертификата на момент оказания услуги;

в случае положительных результатов всех проверок издать атрибутный сертификат в соответствии с политикой применения атрибутных сертификатов;

сохранить все исходные данные, представленные заявителем для издания атрибутного сертификата, и результаты проверки действительности сертификата;

1.3. установление доверия к сертификату, изданному поставщиком услуг иностранного государства, осуществляется республиканским унитарным предприятием «Национальный центр электронных услуг» (далее – предприятие) и включает в себя оценку:

порядка выработки, хранения, резервного копирования, восстановления, депонирования, использования личного ключа электронной цифровой подписи;

порядка регистрации конечных пользователей, издания сертификатов и списков отозванных сертификатов, отзыва, приостановления, возобновления действия сертификатов, предоставления информации о статусе сертификатов;

наличия инфраструктуры, необходимой для оказания услуг по управлению сертификатами;

используемых средств электронной цифровой подписи, криптографических алгоритмов и механизмов, протоколов информационного взаимодействия, форматов обмена данными;

управления операционной деятельностью, системным доступом, внедрением и обслуживанием безопасных доверенных информационных систем, восстановлением при сбоях и обеспечением непрерывности деятельности, безопасностью персонала, физической защитой и защитой от воздействий окружающей среды, защитой информации с учетом актуальных угроз безопасности информации и действий нарушителя в соответствии с законодательством иностранного государства;

порядка и условий прекращения деятельности поставщика услуг иностранного государства.

По результатам оценки предприятием с поставщиком услуг иностранного государства заключается соглашение об установлении доверия к издаваемым им сертификатам.

Предприятие по согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь разрабатывает и утверждает регламент доверенной третьей стороны, в котором определяется порядок взаимодействия с поставщиком услуг иностранного государства и субъектами информационного взаимодействия Республики Беларусь, проведения процедур проверки подлинности электронной цифровой подписи, требования к техническому, программному, информационному взаимодействию, а также меры по защите информации.

2. Внести изменения в следующие приказы Оперативно-аналитического центра при Президенте Республики Беларусь:

2.1. в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 29 ноября 2013 г. № 89 «Об утверждении 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»:

преамбулу изложить в следующей редакции:

«На основании части седьмой статьи 29 Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» ПРИКАЗЫВАЮ:»;

в 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 этим приказом:

в пункте 1 слова «в соответствии с пунктом 3 Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» (Национальный реестр правовых актов Республики Беларусь, 2011 г., № 125, 1/13064)» заменить словами «на основании части седьмой статьи 29 Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи» »;

пункт 2 изложить в следующей редакции:

«2. Для целей настоящей Инструкции применяются термины и их определения в значениях, установленных Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи», техническими нормативными правовыми актами в сфере защиты информации.»;

из части третьей пункта 9 слова «и печатью» исключить;

в приложении 1 к этой Инструкции:

в пункте 2:

подпункты 2.3.2, 2.3.2.1 и 2.3.2.2 изложить в следующей редакции:

«2.3.2. программно-аппаратные средства ЭЦП, используемые для генерации личного ключа подписи УЦ, выработки и проверки ЭЦП при издании сертификатов открытых ключей (далее – ПАС ЭЦП):

2.3.2.1. должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) на соответствие следующим взаимосвязанным с данным техническим регламентом государственным стандартам:

СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности», СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности», где в качестве основы для оценки ПАС ЭЦП используется задание по безопасности с учетом функциональных и гарантийных требований безопасности согласно таблице 3 приложения к Положению о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации, утвержденному приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62;

СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»;

СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» (разделы 6, 7 и 8);

СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»;

СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности» (подраздел 6.9 раздела 6);

СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (подразделы 6.2 и 6.3 раздела 6, подраздел 7.1 раздела 7, таблица Б1 приложения Б, приложение Д);

СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (подраздел 6.1 раздела 6);

СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»;

СТБ 34.101.77-2016 «Информационные технологии и безопасность. Алгоритмы хэширования»;

2.3.2.2. должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь на соответствие требованиям СТБ 34.101.60-2013 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, таблица А1 приложения А) для защиты личного ключа подписи УЦ»;»;

из абзаца шестого подпункта 2.8 слова «(Национальный реестр правовых актов Республики Беларусь, 2007 г., № 262, 1/9048)» исключить;

абзац шестой подпункта 2.9 изложить в следующей редакции:

«источник резервного электропитания должен быть подключен к потребителям электропитания и обеспечивать автоматическую подачу необходимого электроснабжения в течение 30 минут после отключения общегородской сети электроснабжения (источник резервного электропитания не требуется при наличии двух вводов в здание УЦ от различных подстанций);»;

подпункт 2.12 изложить в следующей редакции:

«2.12. пожарная безопасность помещений УЦ должна обеспечиваться в соответствии с нормами и требованиями ТНПА.»;

в пункте 3:

подпункт 3.3.2 изложить в следующей редакции:

«3.3.2. ПАС ЭЦП, которые должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента ТР 2013/027/BY на соответствие взаимосвязанным с данным техническим регламентом государственным стандартам, указанным в подпункте 2.3.2.1 пункта 2 настоящего приложения;»;

абзац четвертый подпункта 3.3.3.1 дополнить словами «(за исключением РЦ, реализующих функции по достоверному подтверждению полномочий, предоставленных физическому лицу от имени организации или другого физического лица)»;

во втором предложении подпункта 3.7 слово «размещения» заменить словами «помещения, а также в случае организации дополнительных переносных рабочих мест сотрудников РЦ для реализации его функций при выезде к заявителю»;

абзац шестой подпункта 3.8 изложить в следующей редакции:

«здание, в котором размещены ТС РЦ, должно находиться под охраной в соответствии с Указом Президента Республики Беларусь от 25 октября 2007 г. № 534;»;

подпункт 3.10 изложить в следующей редакции:

«3.10. пожарная безопасность помещений РЦ должна обеспечиваться в соответствии с нормами и требованиями ТНПА.»;

в приложении 2 к этой Инструкции текст:

«Руководитель организации _____ _____
(подпись) (инициалы, фамилия)
__.__.20__ М.П.»

заменить текстом:

«Руководитель организации _____ _____
(подпись) (инициалы, фамилия)
__.__.20__»;

в приложении 3 к этой Инструкции:

подпункт 3.2 пункта 3 изложить в следующей редакции:

«3.2. копии сертификатов соответствия, выданных в Национальной системе подтверждения соответствия Республики Беларусь, на соответствие программно-аппаратных средств электронной цифровой подписи (далее – ЭЦП), используемых для генерации личного ключа подписи УЦ, выработки и проверки ЭЦП при издании сертификатов открытых ключей, требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) с взаимосвязанными с данным техническим регламентом государственными стандартами, указанными в подпункте 2.3.2.1 пункта 2 приложения 1 к 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;»;

в пункте 4:

подпункт 4.1 исключить;

в подпункте 4.3 слова «в подпункте 3.3.2 пункта 3 приложения 1 к настоящему приказу, и СТБ 34.101.49-2012» заменить словами «в подпункте 2.3.2.1 пункта 2 приложения 1 к 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»;

из приложения 4 к этой Инструкции слова «(Национальный правовой Интернет-портал Республики Беларусь, 06.12.2013, 7/2650)» исключить;

в приложении 6 к этой Инструкции:

подпункт 4.2 пункта 4 изложить в следующей редакции:

«4.2. выполнять функции и обязанности удостоверяющего центра (регистрационного центра), определенные Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118;»;

текст:

«Руководитель аккредитованного
поставщика услуг

_____ _____
(подпись) (инициалы, фамилия)

__. __.20__
М.П.»

заменить текстом:

«Руководитель аккредитованного
поставщика услуг

_____ _____
(подпись) (инициалы, фамилия)

__. __.20__»;

2.2. в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118 «Об утверждении Положения о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь»:

преамбулу изложить в следующей редакции:

«На основании части пятой статьи 29 Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» ПРИКАЗЫВАЮ:»;

Положение о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденное этим приказом, изложить в новой редакции (прилагается).

3. Настоящий приказ вступает в силу с 18 февраля 2019 г.

Начальник **А.Ю.Павлюченко**

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
10.12.2015 № 118
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
08.02.2019 № 45)

ПОЛОЖЕНИЕ
о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

1. Настоящим Положением определяется порядок функционирования Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК).

2. Для целей настоящего Положения термины и их определения используются в значениях, установленных Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи», 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», техническими нормативными правовыми актами, а также следующие термины и их определения:

регистрационный центр – поставщик услуг достоверного подтверждения принадлежности открытого ключа проверки электронной цифровой подписи (далее – открытый ключ) определенным организации или физическому лицу, в том числе индивидуальному предпринимателю (далее, если не предусмотрено иное, – физическое лицо), а также полномочий, предоставленных физическому лицу от имени организации или другого физического лица;

удостоверяющий центр – поставщик услуг издания, распространения, хранения сертификатов открытых ключей (далее – сертификат) и списков отозванных сертификатов, предоставления информации о действительности сертификатов, их отзыва, проставления штампа времени, выработки личных ключей для организаций или физических лиц;

центр атрибутных сертификатов – поставщик услуг издания, распространения, хранения атрибутных сертификатов и списков отозванных атрибутных сертификатов, предоставления информации о действительности атрибутных сертификатов, их отзыва.

3. ГосСУОК осуществляет распространение открытых ключей в виде сертификатов.

Поставщики услуг в ГосСУОК, выполняющие функции удостоверяющих и регистрационных центров, должны иметь специальное разрешение (лицензию) на осуществление деятельности по технической и (или) криптографической защите информации в части составляющих данный вид деятельности работ (услуг).

4. Конечными пользователями ГосСУОК выступают физические лица и организации, которые являются владельцами сертификатов, атрибутных сертификатов и (или) доверяющими сторонами.

5. Функции оператора корневого и республиканского удостоверяющих центров осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее – НЦЭУ).

6. Корневой удостоверяющий центр является базовым компонентом ГосСУОК и занимает высшее положение в единой иерархической инфраструктуре доверия открытых ключей, реализуемой ГосСУОК.

Порядок функционирования корневого удостоверяющего центра и процедура издания самоподписанного сертификата определяются политикой применения сертификатов, разработанной НЦЭУ и утвержденной Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

7. Основными функциями корневого удостоверяющего центра являются:

генерация личных и открытых ключей корневого удостоверяющего центра;

издание, распространение, предоставление информации о статусе, отзыв, хранение самоподписанного сертификата как начала маршрута сертификации (точки доверия) ГосСУОК;

издание, распространение, предоставление информации о статусе, отзыв и хранение сертификата (далее – управление сертификатами) республиканского удостоверяющего центра;

кросс-сертификация (установление отношений доверия) с внешними инфраструктурами открытых ключей, в том числе с иностранными.

8. Основными функциями республиканского удостоверяющего центра являются:

генерация личных и открытых ключей республиканского удостоверяющего центра;

управление сертификатами физических лиц и организаций, в том числе государственных органов и других государственных организаций, регистрационных центров, центра атрибутных сертификатов, службы предоставления информации о действительности сертификатов (OCSP-сервер) и атрибутных сертификатов, службы штампа времени, службы заверения данных, доверенной третьей стороны, сервера идентификации, TLS;

удостоверение формы внешнего представления электронных документов на бумажном носителе.

Также республиканский удостоверяющий центр может осуществлять функции центра атрибутных сертификатов и регистрационного центра.

Республиканский удостоверяющий центр осуществляет согласование регламентов работы регистрационных центров, присоединившихся к политике применения его сертификатов, и инструктаж их персонала.

Реализация функций республиканского удостоверяющего центра по управлению сертификатами осуществляется НЦЭУ на договорной основе.

9. Управление сертификатами, издаваемыми республиканским удостоверяющим центром, функционирование служб предоставления информации о действительности сертификатов (OCSP-сервер) и атрибутных сертификатов, штампа времени, заверения данных, доверенной третьей стороны, идентификации, TLS осуществляются в соответствии с политиками применения сертификатов республиканского удостоверяющего центра, разработанными и утвержденными НЦЭУ по согласованию с ОАЦ.

Порядок действий республиканского удостоверяющего центра, принимаемые организационные и технические меры при издании, управлении, отзыве и обновлении сертификатов отражаются в регламенте, разработанном и утвержденном НЦЭУ по согласованию с ОАЦ.

10. Личные ключи корневого и республиканского удостоверяющих центров должны храниться в тайне и использоваться в сертифицированных программно-аппаратных или аппаратных средствах электронной цифровой подписи.

11. Открытый ключ республиканского удостоверяющего центра распространяется в виде сертификата, изданного корневым удостоверяющим центром.

12. Корневой и республиканский удостоверяющие центры обязаны:

обеспечивать физический доступ к оборудованию, используемому для издания и отзыва сертификатов, только уполномоченным лицам;

разрабатывать и утверждать планы восстановления при сбоях и обеспечения непрерывности деятельности, содержащие описание всех типов сбоев, влияющих на оказание услуг по распространению открытых ключей;

располагать необходимой материально-технической базой, позволяющей надлежащим образом обеспечивать выполнение политик применения сертификатов.

13. Регистрационные центры осуществляют проверку информации, вносимой в сертификаты и атрибутные сертификаты, формирование и регистрацию заявок на издание и отзыв сертификатов и атрибутных сертификатов, передачу конечным пользователям изданных сертификатов и атрибутных сертификатов, обеспечение их взаимодействия с республиканским удостоверяющим центром.

При формировании заявки в республиканский удостоверяющий центр на издание или отзыв сертификатов регистрационный центр должен проверить личность физического лица (данные о государственной регистрации организации), а также полноту и точность представленных данных согласно политике применения сертификатов республиканского удостоверяющего центра и регламенту регистрационного центра.

При формировании заявки в центр атрибутных сертификатов на издание и отзыв атрибутного сертификата регистрационный центр должен проверить:

связь физического лица, являющегося владельцем личного ключа, с организацией или физическим лицом, от имени которых этому физическому лицу предоставлены полномочия на подписание определенных видов электронных документов и (или) иные полномочия (далее, если не предусмотрено иное, – полномочия);

информацию о заявителе, предоставляющем полномочия физическому лицу, и сами эти полномочия.

Регистрационные центры осуществляют свою деятельность в соответствии с регламентом работы, согласованным с республиканским удостоверяющим центром.

14. Владельцем сертификата является организация или физическое лицо, являющееся владельцем личного ключа, на базе которого выработан открытый ключ, значение которого включено в этот сертификат.

15. Республиканский удостоверяющий центр или регистрационный центр обязан предоставить конечным пользователям сертификаты республиканского и корневого удостоверяющих центров.

16. Владельцы сертификатов обязаны:

гарантировать, что вся информация, предоставляемая для издания 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 уведомляется владелец сертификатов;

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.

17. Информация, однозначно идентифицирующая владельца открытого ключа, содержащаяся в сертификате физического лица, издаваемом республиканским удостоверяющим центром, включает в себя фамилию, имя, отчество (если таковое имеется) на государственных языках Республики Беларусь и его идентификационный номер.

В сертификат организаций, в том числе государственных органов и иных государственных организаций, издаваемый республиканским удостоверяющим центром, включается наименование этой организации в соответствии с записями в Едином

государственном регистре юридических лиц и индивидуальных предпринимателей, а также учетный номер плательщика.

18. На основании сертификатов физических лиц, работающих в государственных органах и других государственных организациях, а также иных физических лиц центр атрибутных сертификатов издает атрибутные сертификаты в соответствии с политикой применения атрибутных сертификатов. В атрибутных сертификатах содержится информация о полномочиях таких физических лиц.

Политика применения атрибутных сертификатов разрабатывается и утверждается НЦЭУ по согласованию с ОАЦ.

19. Доверяющие стороны могут запрашивать в республиканском удостоверяющем центре сертификаты и атрибутные сертификаты любого пользователя ГосСУОК и использовать их для проверки электронной цифровой подписи электронного документа.

Перед установлением доверия к электронному документу доверяющие стороны обязаны:

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 на подписание электронного документа определенного типа.

20. Пользователи ГосСУОК вправе получать и осуществлять проверку действительности как собственных сертификатов и атрибутных сертификатов, так и сертификатов и атрибутных сертификатов других пользователей ГосСУОК.

21. Для отзыва сертификата и (или) атрибутного сертификата его владелец взаимодействует с регистрационным центром или с республиканским удостоверяющим центром либо с центром атрибутных сертификатов в соответствии с регламентом республиканского удостоверяющего центра. После рассмотрения заявки на отзыв сертификата и (или) атрибутного сертификата регистрационный центр направляет запрос на его отзыв в республиканский удостоверяющий центр или центр атрибутных сертификатов.

Республиканский удостоверяющий центр (центр атрибутных сертификатов) рассматривает запрос на отзыв сертификата и (или) атрибутного сертификата и в случае принятия решения об отзыве помещает информацию о таком сертификате в список отозванных сертификатов в срок, установленный в политике применения сертификатов и регламенте республиканского удостоверяющего центра.

22. Информационные системы, используемые корневым удостоверяющим центром, республиканским удостоверяющим центром и регистрационными центрами, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, должны иметь аттестованную в установленном порядке систему защиты информации.