

ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ БЕЛАРУСЬ

29 мая 2026 г. № 102

**О 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 26¹, 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. Утвердить:

Инструкцию о порядке проверки принадлежности личного ключа электронной цифровой подписи и издания атрибутного сертификата (прилагается);

Положение о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (прилагается);

Инструкцию о порядке проведения аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (прилагается).

2. Признать утратившими силу:

приказ 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»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2015 г. № 48 «О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 ноября 2013 г. № 89»;

приказ 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»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 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»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 9 октября 2019 г. № 336 «О мерах по реализации Указа Президента Республики Беларусь от 2 сентября 2019 г. № 326»;

подпункты 3.3 и 3.4 пункта 3 приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

пункт 2 приложения 3 к приказу Оперативно-аналитического центра при Президенте Республики Беларусь от 29 декабря 2022 г. № 210 «О реализации Закона Республики Беларусь от 14 октября 2022 г. № 213-З «О лицензировании».

3. Аккредитация поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь по заявкам, поданным до вступления в силу настоящего приказа, осуществляется в порядке, установленном законодательством, действовавшим на дату подачи этих заявок (далее в настоящем пункте – законодательство). Соглашения с поставщиками услуг, аккредитованными на основании указанных заявок, не заключаются. Такие поставщики услуг обеспечивают выполнение обязанностей, предусмотренных в пункте 24 Инструкции о порядке проведения аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденной настоящим приказом (далее в настоящем пункте – Инструкция), и условий аккредитации, определенных законодательством. Аттестаты аккредитации таких поставщиков услуг выдаются по форме согласно приложению 4 к Инструкции.

Соглашения с аккредитованными поставщиками услуг, заключенные до вступления в силу настоящего приказа, прекращают действие со дня вступления его в силу.

Поставщики услуг, аккредитованные до вступления в силу настоящего приказа, обеспечивают выполнение обязанностей, предусмотренных в пункте 24 Инструкции, и условий аккредитации, определенных законодательством. Аттестаты аккредитации, выданные до вступления в силу настоящего приказа, действуют в течение срока, на который они выданы. Изменение, продление срока действия, приостановление (возобновление), прекращение действия таких аттестатов аккредитации осуществляются в порядке, установленном Инструкцией.

4. Настоящий приказ вступает в силу через месяц после его официального опубликования.

Начальник

А.Ю.Павлюченко

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
29.05.2026 № 102

ИНСТРУКЦИЯ

о порядке проверки принадлежности личного ключа электронной цифровой подписи и издания атрибутного сертификата

1. Настоящей Инструкцией определяется порядок проверки принадлежности личного ключа электронной цифровой подписи (далее – личный ключ) его владельцу, издания

атрибутного сертификата, а также подтверждения действительности электронной цифровой подписи, выработанной в соответствии с законодательством иностранного государства.

2. Для целей настоящей Инструкции применяются термины в значениях, определенных в Законе Республики Беларусь «Об электронном документе и электронной цифровой подписи», а также следующие термины и их определения:

оператор доверенной третьей стороны – определенная Президентом Республики Беларусь организация, осуществляющая функции по признанию подлинности электронных документов при межгосударственном электронном взаимодействии;

квитанция доверенной третьей стороны – электронный документ, созданный оператором доверенной третьей стороны и подписанный электронной цифровой подписью такого оператора, служащий для подтверждения результата проверки электронной цифровой подписи в электронном документе.

3. 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 – открытый ключ), личный ключ которого заявитель выработал самостоятельно (без использования технических средств регистрационного центра) с помощью сертифицированного средства электронной цифровой подписи, поставщику услуг представляется информация в соответствии с политикой применения сертификатов открытых ключей поставщика услуг и запрос на получение сертификата открытого ключа, подписанный с использованием личного ключа заявителя (далее – запрос), открытый ключ которого указан в запросе.

Для подтверждения владения заявителем личным ключом поставщиком услуг проверяются:

полнота и точность представленной заявителем информации, личность физического лица, сведения о государственной регистрации индивидуального предпринимателя или организации согласно политике применения сертификатов открытых ключей поставщика услуг;

соответствие информации, указанной в запросе, сформированном заявителем с использованием сертифицированного средства электронной цифровой подписи, представленной заявителем;

уровень стойкости открытого ключа, указанного в запросе, который не должен превышать уровня стойкости открытого ключа удостоверяющего центра;

электронная цифровая подпись, которой подписан запрос, с использованием указанного в нем открытого ключа.

После получения положительного результата проверки поставщик услуг подписывает запрос электронной цифровой подписью.

В случае подтверждения подлинности и целостности запроса считается, что заявитель владеет личным ключом.

4. При обращении к поставщику услуг за изданием атрибутного сертификата заявителем представляются:

заявление на издание атрибутного сертификата;

документ, удостоверяющий личность физического лица, которому от имени заявителя предоставлены полномочия на подписание определенных видов электронных документов, а также иные полномочия (далее – полномочия);

сертификат открытого ключа физического лица, являющегося владельцем этого сертификата, с которым будет связан атрибутный сертификат;

документы, которыми подтверждаются полномочия, предоставленные физическому лицу от имени заявителя, а также статус руководителя (если заявителем является руководитель организации).

5. Документы и информация, указанные в абзацах втором, четвертом и пятом пункта 4 настоящей Инструкции, могут быть представлены в виде электронного документа, подписанного электронной цифровой подписью заявителя.

6. Для издания атрибутного сертификата поставщиком услуг проверяются:

полнота и точность представленных заявителем документов и информации, личность физического лица, сведения о государственной регистрации индивидуального предпринимателя или организации согласно политике применения атрибутных сертификатов поставщика услуг;

наличие документов, которыми подтверждаются полномочия, предоставленные физическому лицу от имени заявителя, а также статус руководителя (если заявителем является руководитель организации);

принадлежность сертификата открытого ключа физическому лицу, которому предоставлены полномочия, а также действительность этого сертификата на момент проверки;

срок действия издаваемого атрибутного сертификата, который не должен превышать срока действия сертификата открытого ключа, с которым он связан.

После получения положительного результата проверки поставщик услуг издает атрибутный сертификат в соответствии с политикой применения атрибутных сертификатов и обеспечивает хранение информации, представленной заявителем для издания атрибутного сертификата, включая результаты проверки действительности сертификата открытого ключа.

7. При установлении доверенной третьей стороной доверия к иностранному сертификату, соответствующего требованиям законодательства иностранного государства, в котором этот сертификат издан, проверка действительности электронной цифровой подписи в электронном документе осуществляется оператором этой доверенной третьей стороны.

По результатам проверки действительности электронной цифровой подписи формируется квитанция доверенной третьей стороны, которая может использоваться в качестве факта признания (непризнания) действительности электронной цифровой подписи в электронном документе, выработанной в соответствии с законодательством иностранного государства.

Оператором доверенной третьей стороны по согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь утверждается регламент доверенной третьей стороны, в котором определяется порядок взаимодействия этого оператора с поставщиками услуг иностранных государств, оценки используемой этими поставщиками для оказания услуг инфраструктуры открытых ключей, взаимодействия оператора доверенной третьей стороны с субъектами информационных отношений Республики Беларусь, проведения процедур проверки действительности электронной цифровой подписи, требования к техническому, программному и информационному взаимодействию, а также меры по защите информации.

Оператором доверенной третьей стороны заключается с поставщиком услуг иностранного государства соглашение об установлении доверия к издаваемым таким поставщиком сертификатам, в котором определяются используемые средства электронной цифровой подписи, криптографические алгоритмы и порядок информационного взаимодействия.

Соглашение, указанное в части четвертой настоящего пункта, подлежит согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
29.05.2026 № 102

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 применяются термины в значениях, определенных в Законе Республики Беларусь «Об электронном документе и электронной цифровой подписи», Положении о технической и криптографической защите информации, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, а также следующие термины и их определения:

регистрационный центр – поставщик услуг по достоверному подтверждению 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 предоставленных физическому лицу от имени организации или другого физического лица полномочий на подписание определенных видов электронных документов и (или) иных полномочий (далее, если не предусмотрено иное, – полномочия);

удостоверяющий центр – поставщик услуг по изданию, распространению, хранению сертификатов открытых ключей и списков отозванных сертификатов открытых ключей, предоставлению информации о действительности сертификатов открытых ключей, отзыву сертификатов открытых ключей, проставлению штампа времени, выработке личных ключей электронной цифровой подписи (далее – личный ключ) для организаций или физических лиц;

центр атрибутных сертификатов – поставщик услуг по изданию, распространению, хранению атрибутных сертификатов и списков отозванных атрибутных сертификатов, предоставлению информации о действительности атрибутных сертификатов, отзыву атрибутных сертификатов.

3. В ГосСУОК распространение открытых ключей осуществляется в виде сертификатов открытых ключей.

4. Конечными пользователями ГосСУОК выступают организации или физические лица, которые являются владельцами сертификатов открытых ключей, атрибутивных 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 занимает высшее положение в единой иерархической инфраструктуре доверия открытых ключей, реализуемой ГосСУОК.

Порядок издания, распространения, хранения сертификатов открытых ключей и списков отозванных сертификатов открытых ключей, предоставления информации о действительности сертификатов открытых ключей, отзыва сертификатов открытых ключей (далее – управление сертификатами) корневого удостоверяющего центра определяется политикой применения сертификатов открытых ключей.

Порядок функционирования корневого удостоверяющего центра при управлении сертификатами, включая организационные и технические меры, определяется в регламенте.

Документы, указанные в частях второй и третьей настоящего пункта, утверждаются НЦЭУ по согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

7. Корневой удостоверяющий центр осуществляет:

выработку личных и открытых ключей корневого удостоверяющего центра;

хранение личных ключей корневого удостоверяющего центра;

управление сертификатами корневого удостоверяющего центра как начала маршрута доверия (точки доверия) ГосСУОК;

управление сертификатами республиканского удостоверяющего центра;

линк-сертификацию (для установления доверия к новому сертификату корневого удостоверяющего центра);

кросс-сертификацию (для установления отношений доверия) с внешними инфраструктурами открытых ключей, в том числе иностранными.

8. Республиканский удостоверяющий центр осуществляет:

выработку личных и открытых ключей республиканского удостоверяющего центра;

хранение личных ключей республиканского удостоверяющего центра;

управление изданными им сертификатами физических лиц и организаций, в том числе государственных органов и иных государственных организаций, регистрационных центров, центра атрибутивных сертификатов, службы предоставления информации о действительности сертификатов открытых ключей и атрибутивных сертификатов (OCSP-сервер), службы штампа времени, службы заверения данных, службы идентификации, доверенной третьей стороны, технологическими сертификатами для средств криптографической защиты информации. Управление сертификатами осуществляется в соответствии с политиками применения сертификатов республиканского удостоверяющего центра, утверждаемыми НЦЭУ по согласованию с ОАЦ;

удостоверение формы внешнего представления электронного документа на бумажном носителе.

Порядок функционирования республиканского удостоверяющего центра при управлении сертификатами, включая организационные и технические меры, определяется в регламенте, который утверждается НЦЭУ по согласованию с ОАЦ (далее – регламент деятельности республиканского удостоверяющего центра).

Республиканский удостоверяющий центр вправе осуществлять функции центра атрибутных сертификатов, регистрационного центра, а также службы штампа времени и предоставления информации о действительности сертификатов открытых ключей, атрибутных сертификатов.

Республиканским удостоверяющим центром осуществляется согласование регламентов деятельности регистрационных центров, присоединившихся к политике применения его сертификатов, и инструктаж персонала таких центров, порядок проведения которого определяется НЦЭУ по согласованию с ОАЦ.

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

9. Личные ключи корневого и республиканского удостоверяющих центров должны храниться в тайне и использоваться в сертифицированных программно-аппаратных средствах криптографической защиты информации.

10. Открытые ключи республиканского удостоверяющего центра распространяются в виде сертификатов открытых ключей, изданных корневым удостоверяющим центром.

11. Корневой и республиканский удостоверяющие центры обязаны:

обеспечивать физический доступ к оборудованию, используемому для управления сертификатами, только уполномоченным лицам;

иметь утвержденные 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.

12. Регистрационные центры осуществляют проверку информации, вносимой в сертификаты открытых ключей и атрибутные сертификаты, формирование и регистрацию запросов на издание сертификатов открытых ключей, прием заявлений на издание или отзыв сертификатов открытых ключей и атрибутных сертификатов, передачу пользователям изданных сертификатов открытых ключей и атрибутных сертификатов, обеспечение их взаимодействия с республиканским удостоверяющим центром.

При формировании запроса на издание и приеме заявления на издание или отзыв сертификатов открытых ключей в республиканский удостоверяющий центр регистрационный центр проверяет информацию о физическом лице, его личность, сведения об организации или индивидуальном предпринимателе, а также полноту и точность представленной информации согласно политике применения сертификатов республиканского удостоверяющего центра и регламенту деятельности регистрационного центра.

При приеме заявления в центр атрибутных сертификатов на издание или отзыв атрибутного сертификата регистрационным центром проверяются:

полнота и точность представленной физическим лицом или организацией (далее – заявитель) информации, личность физического лица, сведения о государственной регистрации

индивидуального предпринимателя или организации согласно политике применения атрибутивных сертификатов;

наличие документов, которыми подтверждаются полномочия, предоставленные физическому лицу от имени заявителя, а также статус руководителя (если заявителем является руководитель организации);

принадлежность сертификата открытого ключа физическому лицу, которому предоставлены полномочия, а также действительность этого сертификата на момент проверки;

срок действия издаваемого атрибутивного сертификата, который не должен превышать срока действия сертификата открытого ключа, с которым он связан.

Заявители несут ответственность за предоставление полных и достоверных данных при подаче документов в регистрационные центры и (или) республиканский удостоверяющий центр.

В ходе проверки данных, указанных в частях второй и третьей настоящего пункта, допускается использование открытых и общедоступных сведений из Единого государственного регистра юридических лиц и индивидуальных предпринимателей, реестра представительств иностранных организаций и филиалов иностранных юридических лиц, Государственного реестра плательщиков (иных обязанных лиц), корпоративного портала Фонда социальной защиты населения Министерства труда и социальной защиты.

Регистрационные центры осуществляют свою деятельность в соответствии с регламентами, согласованными с НЦЭУ.

13. Владельцем сертификата открытого ключа являются организация или физическое лицо, являющиеся владельцем личного ключа, на базе которого выработан открытый ключ, включенный в этот сертификат.

14. Республиканский удостоверяющий центр обязан предоставить конечным пользователям сертификаты открытых ключей республиканского и корневого удостоверяющих центров, а также центра атрибутивных сертификатов.

15. Владельцы сертификатов открытых ключей обязаны:

гарантировать, что вся информация, предоставляемая для издания сертификатов открытых ключей, является полной и достоверной;

хранить в тайне личный ключ;

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

отозвать сертификат открытого ключа в случае, если тайна соответствующего ему личного ключа нарушена;

использовать личный ключ в целях, не противоречащих законодательству;

не использовать личный ключ, если соответствующий ему открытый ключ в виде сертификата открытого ключа отозван или срок действия этого сертификата истек;

выполнять иные обязанности, установленные законодательством об электронном документе и электронной цифровой подписи.

16. Информация, однозначно идентифицирующая владельца открытого ключа, содержащаяся в сертификате открытого ключа физического лица, издаваемом республиканским удостоверяющим центром, включает в себя фамилию, собственное имя,

отчество (если таковое имеется) на одном из государственных языков Республики Беларусь и его идентификационный номер (данные), указанные в документе, удостоверяющем личность.

В сертификаты открытых ключей организаций, в том числе государственных органов и иных государственных организаций, индивидуальных предпринимателей, издаваемые республиканским удостоверяющим центром, включаются наименования этих организаций или индивидуальных предпринимателей, а также учетный номер плательщика в соответствии с записями в свидетельстве о государственной регистрации организации или индивидуального предпринимателя, ином документе, предусмотренном законодательством, либо их копиях, заверенных в установленном порядке.

17. Центр атрибутных сертификатов издает атрибутные сертификаты в соответствии с политикой применения атрибутных сертификатов. Атрибутные сертификаты применяются совместно с сертификатами открытых ключей физических лиц и содержат информацию о полномочиях таких физических лиц.

Политика применения атрибутных сертификатов утверждается НЦЭУ по согласованию с ОАЦ.

18. Доверяющие стороны могут запрашивать в республиканском удостоверяющем центре сертификаты открытых ключей и атрибутные сертификаты любого пользователя ГосСУОК для использования их при проверке электронной цифровой подписи в электронном документе.

Перед установлением доверия к электронному документу доверяющие стороны обязаны:

- проверить действительность сертификата открытого ключа, атрибутного сертификата, в том числе на отзыв;

- установить связь атрибутного сертификата с сертификатом открытого ключа;

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

19. Пользователи ГосСУОК вправе получать собственные сертификаты открытых ключей и атрибутные сертификаты, сертификаты открытых ключей и атрибутные сертификаты других пользователей ГосСУОК, предоставленные поставщиком услуг на основании запроса или их владельцами.

20. Для отзыва сертификата открытого ключа и (или) атрибутного сертификата его (их) владелец взаимодействует с регистрационным центром или с республиканским удостоверяющим центром либо с центром атрибутных сертификатов в соответствии с политикой применения сертификатов и регламентом деятельности республиканского удостоверяющего центра. После рассмотрения заявления на отзыв сертификата открытого ключа и (или) атрибутного сертификата регистрационный центр направляет запрос на его (их) отзыв в республиканский удостоверяющий центр и (или) центр атрибутных сертификатов.

Отзыв сертификатов открытых ключей и (или) атрибутных сертификатов может быть инициирован лицами, не являющимися владельцами таких сертификатов, в случаях, предусмотренных законодательными актами.

Республиканский удостоверяющий центр и (или) центр атрибутных сертификатов проверяют запрос на отзыв сертификата открытого ключа и (или) атрибутного сертификата и в случае принятия решения об отзыве включают информацию о таком сертификате в список

отозванных сертификатов в установленный политикой применения сертификатов и регламентом деятельности республиканского удостоверяющего центра срок.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
29.05.2026 № 102

ИНСТРУКЦИЯ

**о порядке проведения аккредитации в Государственной системе
управления открытыми ключами проверки электронной цифровой
подписи Республики Беларусь**

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящей Инструкцией устанавливается порядок проведения Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – орган по аккредитации) аккредитации поставщиков услуг (далее, если не установлено иное, – заявитель) в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК), выдачи, продления срока действия, приостановления (возобновления), прекращения действия, изменения аттестата аккредитации и осуществления контроля за соблюдением условий аккредитации.

2. Для целей настоящей Инструкции применяются термины в значениях, определенных в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Законе Республики Беларусь «Об электронном документе и электронной цифровой подписи» и Положении о технической и криптографической защите информации, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196.

3. В ходе аккредитации поставщиков услуг в ГосСУОК (далее – аккредитация) осуществляется оценка заявителей на соответствие условиям аккредитации согласно приложению 1.

4. Для проведения аккредитации заявителем представляется в орган по аккредитации заявление по форме согласно приложению 2, к которому прилагаются документы (сведения) по перечню согласно приложению 3.

Прилагаемые к заявлению документы (сведения) представляются на одном из государственных языков Республики Беларусь либо на языке оригинала с переводом на один из государственных языков Республики Беларусь, заверенным в установленном порядке.

5. Заявление с прилагаемыми к нему документами (сведениями) может быть подано в орган по аккредитации лично заявителем (его представителем) либо направлено с использованием системы межведомственного электронного документооборота государственных органов Республики Беларусь (далее – СМДО), общегосударственной

автоматизированной информационной системы (далее – ОАИС) (при наличии технической возможности), посредством почтовой связи.

Личное представление заявления с прилагаемыми к нему документами (сведениями) осуществляется заявителем (его представителем) с одновременным предъявлением:

документа, удостоверяющего личность, и документа, подтверждающего полномочия руководителя (приказ о назначении на должность руководителя, выписка из решения общего собрания, правления либо иного органа управления юридического лица, трудовой договор (контракт), гражданско-правовой договор, иной документ в соответствии с законодательством), – руководителем заявителя;

документа, удостоверяющего личность, доверенности или иного документа, подтверждающего полномочия на совершение юридически значимых действий от имени заявителя, – уполномоченным представителем заявителя.

Подаваемое на бумажном носителе в орган по аккредитации заявление и прилагаемые к нему документы (копии документов) должны быть подписаны (заверены в установленном порядке).

6. В принятии заявления отказывается:

в случае нахождения заявителя в процессе ликвидации;

в случаях указания в заявлении неполных сведений либо представления не всех документов (сведений), предусмотренных настоящей Инструкцией.

Мотивированный отказ в принятии заявления не позднее семи рабочих дней, следующих за днем его поступления, вместе с этим заявлением и прилагаемыми к нему документами (сведениями) направляется заявителю с использованием СМДО, либо ОАИС (при наличии технической возможности), либо почтовой связи.

Заявитель вправе повторно подать заявление в орган по аккредитации после устранения недостатков, явившихся причиной отказа в его приеме.

7. В случае принятия к рассмотрению заявления и приложенных к нему документов (сведений) с заявителем заключается договор на проведение аккредитации.

8. Аккредитация включает следующие этапы:

заключение договора на проведение аккредитации;

изучение и анализ имеющихся в органе по аккредитации представленных заявителем и полученных при необходимости от иных государственных органов и других организаций документов (сведений), подтверждающих соответствие заявителя условиям аккредитации;

проведение оценки заявителя на соответствие условиям аккредитации (далее – оценка заявителя);

оформление отчета об аккредитации;

выдача аттестата аккредитации по форме согласно приложению 4.

9. Изучение и анализ заявления с прилагаемыми к нему документами (сведениями) проводятся органом по аккредитации в течение 20 рабочих дней со дня, следующего за днем подписания договора последней из сторон.

10. Сведения, полученные сторонами при исполнении договора на проведение аккредитации, являются конфиденциальными. Заявитель и орган по аккредитации принимают необходимые меры по обеспечению защиты полученных конфиденциальных сведений.

11. Орган по аккредитации ведет реестр поставщиков услуг, аккредитованных в ГосСУОК (далее – реестр), который содержит актуальную информацию о выданных аттестатах аккредитации, текущем состоянии аттестата аккредитации поставщика услуг.

Реестр размещается на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет.

ГЛАВА 2

ОЦЕНКА ЗАЯВИТЕЛЯ

12. Решение о проведении оценки заявителя принимается руководителем органа по аккредитации в форме приказа, которым назначается экспертная группа и определяется ее персональный состав.

В состав экспертной группы включаются представители органа по аккредитации, а также при необходимости оператора, осуществляющего функции корневого и республиканского удостоверяющих центров ГосСУОК, и технические эксперты.

13. Оценка заявителя проводится с выездом на место оказания услуг.

14. Экспертная группа в ходе оценки заявителя проверяет:

возможности заявителя по оказанию услуг (в качестве удостоверяющего центра и (или) регистрационного центра по распространению открытых ключей проверки электронной цифровой подписи (далее – открытые ключи);

соответствие условиям аккредитации в качестве удостоверяющего центра и (или) регистрационного центра.

Оценка заявителя, который планирует оказывать услуги в качестве удостоверяющего центра и (или) регистрационного центра, проводится посредством моделирования процесса оказания услуг по распространению открытых ключей: выработка, хранение, резервное копирование и восстановление личного ключа электронной цифровой подписи (далее – личный ключ) удостоверяющего центра; формирование и регистрация запросов на издание сертификатов открытых ключей, прием заявлений на издание или отзыв сертификатов открытых ключей и атрибутивных сертификатов, передача пользователям изданных сертификатов открытых ключей и атрибутивных сертификатов, обеспечение их взаимодействия с удостоверяющим центром; издание сертификатов открытых ключей и списков отозванных сертификатов открытых ключей, атрибутивных сертификатов и списков отозванных атрибутивных сертификатов; отзыв, обновление данных сертификатов открытых ключей и атрибутивных сертификатов.

15. Основаниями для отказа в аккредитации являются:

наличие в заявлении и прилагаемых к нему документах (сведениях) недостоверной (не соответствующей действительности) информации;

письменный отказ заявителя от проведения аккредитации;

несоответствие заявителя условиям аккредитации.

16. По результатам оценки заявителя оформляется отчет об аккредитации, который подписывается членами экспертной группы и утверждается руководителем органа по аккредитации или уполномоченным им заместителем.

При отсутствии у заявителя недостатков в отчете об аккредитации делается вывод о соответствии заявителя условиям аккредитации и выдаче аттестата аккредитации.

В случае выявления в ходе оценки заявителя недостатков информация о них указывается в отчете об аккредитации с перечислением мероприятий, которые необходимо выполнить, о чем письменно уведомляется заявитель.

17. Заявителем в срок, установленный в письменном уведомлении, разрабатывается перечень мероприятий по устранению выявленных недостатков (далее – мероприятия), который представляется на согласование в орган по аккредитации.

О выполнении мероприятий и принятых мерах информируется орган по аккредитации в срок, не превышающий 90 календарных дней с даты согласования мероприятий.

Экспертной группой анализируются выполненные мероприятия на предмет их эффективности и достаточности.

Для проверки выполнения мероприятий орган по аккредитации вправе запросить дополнительную информацию, а также провести дополнительную оценку заявителя.

По результатам анализа и проверки выполненных мероприятий органом по аккредитации оформляется отчет об аккредитации в порядке, установленном в частях первой и второй пункта 16 настоящей Инструкции.

В случае невыполнения заявителем мероприятий органом по аккредитации в отчете об аккредитации делается вывод о несоответствии заявителя условиям аккредитации и отказе в выдаче аттестата аккредитации, о чем письменно уведомляется заявитель.

При невозможности выполнения мероприятий заявителем может быть принято решение об отказе от проведения аккредитации, о чем письменно уведомляется орган по аккредитации.

В случае непредставления заявителем в установленный срок информации о выполнении мероприятий проведение аккредитации прекращается, о чем письменно уведомляется заявитель.

Анализ и проверка выполнения мероприятий, включая проведение дополнительной оценки заявителя, осуществляются органом по аккредитации после подписания дополнительного соглашения к договору на проведение аккредитации.

18. В случае изменения места нахождения поставщика услуг, места оказания услуг, расположения помещений, которые используются для оказания услуг (включая серверные помещения, предназначенные для обеспечения деятельности поставщика услуг), проводится аккредитация поставщика услуг в части произведенных изменений.

В случае увеличения количества рабочих мест, расположенных в одном помещении и используемых для оказания услуг, а также замены технических, программно-аппаратных и программных средств, необходимых для оказания услуг, поставщиком услуг письменно уведомляется об этом орган по аккредитации (с указанием описания корректности настройки и функционирования рабочих мест и (или) средств).

Если поставщик услуг аккредитован в качестве регистрационного центра, к уведомлению дополнительно прилагаются документы, указанные в абзаце шестом пункта 3 приложения 3.

Сокращение количества мест оказания услуг и (или) рабочих мест, используемых для оказания услуг, осуществляется после письменного уведомления об этом органа по аккредитации и внесения соответствующих изменений в аттестат аккредитации.

19. При наличии сведений, свидетельствующих об изменении условий аккредитации, после получения уведомления, предусмотренного в пункте 18 настоящей Инструкции,

органом по аккредитации может быть принято решение об осуществлении контроля за соблюдением условий аккредитации.

ГЛАВА 3

АТТЕСТАТ АККРЕДИТАЦИИ

20. Выдача аттестата аккредитации осуществляется в течение пяти рабочих дней после принятия соответствующего решения органом по аккредитации.

21. Срок действия аттестата аккредитации составляет пять лет.

22. На оборотной стороне аттестата аккредитации указываются:

адрес места нахождения поставщика услуг;

перечень мест оказания услуг с их адресами (при наличии у поставщика услуг структурных подразделений, оказывающих услуги по распространению открытых ключей).

Аттестат аккредитации также может содержать иные сведения.

23. Аттестат аккредитации выдается руководителю поставщика услуг или его уполномоченному представителю под подпись в журнале регистрации и выдачи аттестатов аккредитации.

24. В период действия аттестата аккредитации аккредитованный поставщик услуг обязуется:

соблюдать условия аккредитации;

выполнять функции удостоверяющего и (или) регистрационного центров, определенные Положением о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденным приказом, утвердившим настоящую Инструкцию;

осуществлять распространение открытых ключей в соответствии с политиками применения сертификатов открытых ключей, атрибутных сертификатов, согласованными с органом по аккредитации, и регламентом деятельности удостоверяющего (регистрационного) центра;

обеспечивать беспрепятственный доступ в помещения и на иные объекты (территории), в (на) которых размещено (функционирует) оборудование, используемое для оказания услуг по распространению открытых ключей, а также к программно-техническим средствам, с помощью которых обеспечивается их функционирование, представителям органа по аккредитации, осуществляющим контроль за соблюдением условий аккредитации, оказывать им содействие в его проведении;

письменно информировать орган по аккредитации:

о компрометации личного ключа удостоверяющего центра (регистратора) – незамедлительно;

о возникновении нештатных ситуаций или о нарушениях функционирования удостоверяющего и (или) регистрационного центров – в течение суток;

о планируемых изменениях условий функционирования удостоверяющего и (или) регистрационного центров – не позднее чем за три рабочих дня;

о нарушениях порядка оказания услуг пользователям, с которыми заключены договоры, – в течение пяти рабочих дней с момента установления таких нарушений.

25. Действие аттестата аккредитации может быть приостановлено по следующим основаниям:

наличие недостатков, выявленных по результатам контроля за соблюдением условий аккредитации;

письменное уведомление поставщика услуг о приостановлении деятельности;

невыполнение поставщиком услуг обязанностей, предусмотренных в пункте 24 настоящей Инструкции.

26. Основаниями прекращения действия аттестата аккредитации являются:

ликвидация поставщика услуг;

неосуществление поставщиком услуг деятельности в течение двух лет подряд;

письменное уведомление поставщика услуг о прекращении деятельности;

окончание срока действия аттестата аккредитации;

наличие фактов несоблюдения условий аккредитации, в том числе выявленных при проведении контроля за соблюдением условий аккредитации.

27. Решение о выдаче аттестата аккредитации, отказе в его выдаче, приостановлении (возобновлении) и прекращении действия аттестата аккредитации оформляется приказом органа по аккредитации.

Решение о приостановлении (возобновлении) и прекращении действия аттестата аккредитации может быть принято по результатам осуществления контроля за соблюдением условий аккредитации.

Для приостановления или прекращения действия аттестата аккредитации по основаниям, предусмотренным в абзаце третьем пункта 25 и абзаце четвертом пункта 26 настоящей Инструкции, поставщиком услуг направляется в орган по аккредитации соответствующее письменное уведомление с указанием даты приостановления или прекращения деятельности.

Срок приостановления действия аттестата аккредитации по основанию, предусмотренному в абзаце третьем пункта 25 настоящей Инструкции, не может превышать двух лет.

Письменное уведомление о прекращении поставщиком услуг деятельности направляется не менее чем за 20 календарных дней до предполагаемой даты ее прекращения. При этом аттестат аккредитации возвращается в орган по аккредитации после прекращения поставщиком услуг деятельности.

28. После приостановления (прекращения) действия аттестата аккредитации удостоверяющим центром проводится блокировка соответствующих учетных записей и выполняется комплекс мероприятий, направленных на исключение возможности оказания услуг по распространению открытых ключей.

До прекращения действия аттестата аккредитации поставщик услуг, аккредитованный в качестве регистрационного центра, осуществляет передачу удостоверяющему центру регистрационной информации и записей архивов для хранения.

Для возобновления действия аттестата аккредитации поставщиком услуг направляется в орган по аккредитации письменное уведомление с указанием планируемой даты возобновления деятельности.

29. При необходимости внесения изменений в аттестат аккредитации выдается новый аттестат аккредитации, а ранее выданный возвращается в орган по аккредитации.

30. Аттестат аккредитации подписывается руководителем органа по аккредитации или его уполномоченным заместителем и скрепляется печатью с изображением Государственного герба Республики Беларусь.

31. Информация о выдаче, приостановлении, продлении срока действия аттестата аккредитации, внесенных в него изменениях указывается в реестре.

При прекращении действия аттестата аккредитации сведения о нем подлежат исключению из реестра.

32. В случае продления срока действия аттестата аккредитации осуществляется оценка заявителя.

В целях продления срока действия аттестата аккредитации поставщиком услуг не позднее чем за три месяца до окончания срока его действия направляется заявление в орган по аккредитации.

33. В ходе оценки поставщика услуг в целях продления срока действия аттестата аккредитации помимо мероприятий, указанных в пункте 14 настоящей Инструкции, экспертной группой:

проверяется выполнение условий аккредитации за период действия аттестата аккредитации;

проверяется выполнение поставщиком услуг обязанностей, предусмотренных в пункте 24 настоящей Инструкции;

учитываются результаты предыдущих оценок поставщика услуг, а также контроля за соблюдением условий аккредитации;

анализируется поступившая от государственных органов и иных организаций информация, а также обращения граждан и юридических лиц по вопросам деятельности поставщика услуг.

34. При продлении срока действия аттестата аккредитации новый регистрационный номер аттестату не присваивается, в нем указывается новый срок действия.

35. Действие аттестата аккредитации может быть продлено органом по аккредитации на время проведения аккредитации поставщика услуг, при этом в аттестат аккредитации вносится соответствующая отметка.

ГЛАВА 4

КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ УСЛОВИЙ АККРЕДИТАЦИИ

36. Контроль за соблюдением условий аккредитации осуществляется в форме проверок, проводимых в соответствии с планом проверок, размещаемым на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет не позднее 30 декабря года, предшествующего году проведения проверки.

Без включения в план, указанный в части первой настоящего пункта, проверки могут назначаться руководителем органа по аккредитации при наличии сведений, в том числе полученных от государственных органов, иных организаций или физических лиц, свидетельствующих о совершаемом (совершенном) нарушении условий аккредитации и (или) невыполнении обязанностей, предусмотренных в пункте 24 настоящей Инструкции.

37. Для проведения проверки решением руководителя органа по аккредитации назначается комиссия.

О проведении проверки поставщик услуг письменно уведомляется не позднее десяти рабочих дней до начала ее проведения. Уведомление должно содержать сведения о дате начала проверки, сроках ее проведения, а также о вопросах, подлежащих проверке.

38. Для проведения проверки разрабатывается план проверочных мероприятий, который утверждается руководителем органа по аккредитации или его уполномоченным заместителем.

План проверочных мероприятий доводится руководителю поставщика услуг или его уполномоченному лицу при представлении комиссии.

39. Проверка проводится в порядке, предусмотренном для оценки заявителя, с учетом особенностей, предусмотренных в пунктах 40–42 настоящей Инструкции.

При проведении проверки председатель комиссии самостоятельно определяет методы и способы ее осуществления.

40. По результатам проверки составляется акт проверки в количестве не менее двух экземпляров с указанием в нем выводов о соблюдении поставщиком услуг условий аккредитации.

41. Акт проверки составляется в течение десяти рабочих дней со дня окончания проверки, подписывается членами комиссии и утверждается руководителем органа по аккредитации или его уполномоченным заместителем.

В течение трех рабочих дней после составления акта проверки один экземпляр этого акта направляется поставщику услуг, второй – остается в органе по аккредитации.

42. Недостатки, отмеченные в акте проверки, подлежат устранению поставщиком услуг в установленный в нем срок. Акт проверки также может содержать перечень мероприятий, которые рекомендуется выполнить поставщику услуг (далее – рекомендации).

Об устранении недостатков и выполнении рекомендаций поставщик услуг письменно сообщает в орган по аккредитации в пределах срока, установленного в акте, с приложением подтверждающих документов, а также предоставляет органу по аккредитации возможность удостовериться на месте в устранении нарушений и выполнении рекомендаций.

При наличии объективных обстоятельств, не позволивших устранить нарушения и выполнить рекомендации, указанные в акте проверки, в установленный в нем срок, по заявлению поставщика услуг, поданному не позднее трех рабочих дней до дня истечения этого срока с указанием соответствующих обстоятельств, руководителем органа по аккредитации или его уполномоченным заместителем может быть принято решение о переносе срока устранения нарушений и выполнении рекомендаций.

43. По результатам контроля за соблюдением условий аккредитации возобновление действия приостановленного аттестата аккредитации осуществляется органом по аккредитации после анализа документов, подтверждающих устранение поставщиком услуг недостатков, выполнения рекомендаций, а также при необходимости после проведения дополнительной проверки.

УСЛОВИЯ

аккредитации поставщиков услуг

1. Для аккредитации в ГосСУОК поставщики услуг должны иметь лицензию на осуществление деятельности по технической и (или) криптографической защите информации, составляющими услугами которой являются:

распространение открытых ключей проверки электронной цифровой подписи и удостоверение формы внешнего представления электронного документа на бумажном носителе (для аккредитации в качестве удостоверяющего центра);

распространение открытых ключей проверки электронной цифровой подписи (для аккредитации в качестве регистрационного центра).

2. Аккредитация удостоверяющего центра в ГосСУОК осуществляется на соответствие следующим условиям:

2.1. наличие утвержденных политик применения издаваемых удостоверяющим центром сертификатов открытых ключей, атрибутных сертификатов (далее – политики применения сертификатов) и регламента деятельности удостоверяющего центра;

2.2. реализация требований, указанных в политиках применения сертификатов и регламенте деятельности удостоверяющего центра;

2.3. использование следующих программных, программно-аппаратных и технических средств для реализации услуг и обеспечения деятельности:

2.3.1. системного и прикладного программного обеспечения. При этом:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и при необходимости другое программное обеспечение должны быть приобретены на основании лицензионного договора либо ином законном основании или быть свободно распространяемыми;

системное и прикладное программное обеспечение должно быть установлено, сконфигурировано и находиться в работоспособном состоянии;

в удостоверяющем центре должно использоваться только системное и прикладное программное обеспечение, которое необходимо для функционирования удостоверяющего центра;

2.3.2. технических средств обеспечения функционирования удостоверяющего центра. При этом такие технические средства должны быть исправны, корректно сконфигурированы, работоспособны и включать:

сервер (серверы) удостоверяющего центра;

средства резервного копирования;

источник (устройство) получения точного времени (основной и резервный);

телекоммуникационное оборудование;

электронные вычислительные машины рабочих мест сотрудников удостоверяющего центра;

средства обеспечения бесперебойной работы;
устройства печати на бумажных носителях (принтеры).

При выполнении удостоверяющим центром функций регистрационного центра должны быть дополнительно предусмотрены следующие технические средства:

сервер (серверы) или автоматизированное рабочее место регистрационного центра;

устройства подтверждения подлинности документов, удостоверяющих личность (за исключением корневого удостоверяющего центра).

Технические средства должны обеспечивать возможность непрерывной и бесперебойной работы программного обеспечения удостоверяющего центра, а также производительность (скорость выполнения операций), достаточную для выполнения любой прикладной задачи (услуги удостоверяющего центра) в течение минимум 30 минут;

2.4. наличие системы защиты информации информационной системы удостоверяющего центра, аттестованной в установленном порядке. При этом:

средства защиты информации, используемые в удостоверяющем центре, должны иметь сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 (далее – сертификат соответствия), или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – экспертное заключение);

для выработки личных ключей и открытых ключей, а также для защиты личных ключей удостоверяющего центра должны использоваться программно-аппаратные средства криптографической защиты информации (далее – СКЗИ);

находясь за пределами криптографической границы СКЗИ, личные ключи удостоверяющего центра должны быть защищены таким образом, чтобы обеспечить тот же уровень защиты, который обеспечивается СКЗИ;

активы удостоверяющего центра должны быть настроены таким образом, чтобы обеспечивалось удаление или отключение всех учетных записей, приложений, служб, протоколов и портов, которые не используются при его функционировании;

управление активами удостоверяющего центра посредством внешних информационных потоков должно осуществляться с использованием защищенных каналов передачи данных, обеспечивающих взаимную аутентификацию сторон;

взаимодействие информационной системы удостоверяющего центра с информационными системами регистрационных центров должно осуществляться с использованием защищенных каналов передачи данных;

должна быть обеспечена многофакторная аутентификация с использованием аппаратных носителей ключевой информации для всех учетных записей, которые позволяют инициировать процедуру издания или отзыва сертификатов открытых ключей, атрибутивных сертификатов;

информационная система корневого удостоверяющего центра не должна иметь подключений к внешним информационным потокам;

события с технических средств, связанные с функционированием удостоверяющего центра, должны регистрироваться таким образом, чтобы они не были несанкционированно удалены (за исключением случаев надежного переноса на долговременные носители информации), и подлежать архивному хранению;

события, связанные с выработкой личных и открытых ключей, получением, изданием и отзывом сертификатов открытых ключей, атрибутивных сертификатов, должны храниться в удостоверяющем центре не менее семи лет после того, как названные сертификаты стали недействительными;

2.5. соответствие требованиям по обеспечению безопасности при монтаже, наладке, эксплуатации и обслуживании технических средств удостоверяющего центра документации на соответствующее оборудование;

2.6. размещение серверного и телекоммуникационного оборудования удостоверяющего центра в отдельном или серверном помещении;

2.7. соответствие следующим требованиям по физическому доступу к активам удостоверяющего центра:

физический доступ к активам должен быть предоставлен только уполномоченным лицам и обеспечен системой контроля и управления доступом, осуществляющей проверку разрешения на доступ;

активы должны быть расположены в помещениях, оборудованных охранной сигнализацией и видеонаблюдением;

в системе контроля и управления доступом должны регистрироваться все события, связанные с получением физического доступа к активам и отказом в таком доступе;

охрана объекта, в котором размещены технические средства, должна обеспечивать обнаружение и реагирование на несанкционированный доступ в помещения (установка средств оповещения о несанкционированном доступе, охрана помещений уполномоченной организацией (работником), при этом должен быть определен и утвержден порядок охраны помещений и реагирования ответственных лиц на несанкционированный доступ);

2.8. соответствие следующим требованиям к электроснабжению удостоверяющего центра:

технические средства в повседневном режиме должны быть подключены к электрической сети энергоснабжающей организации;

используемые электрические сети и электрооборудование должны соответствовать требованиям законодательства, в том числе обязательным для соблюдения требованиям технических нормативных правовых актов;

технические средства, включая серверное и телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение времени, необходимого для переключения на резервное электропитание этих технических средств;

в случае прекращения подачи электрической энергии должно быть предусмотрено резервное электропитание технических средств;

источник резервного электропитания должен быть подключен к потребителям электропитания и обеспечивать автоматическую подачу необходимой электрической энергии после прекращения подачи электрической энергии от энергоснабжающей организации в течение времени, регламентированного в эксплуатационной документации;

2.9. оснащение помещения удостоверяющего центра с серверным и телекоммуникационным оборудованием:

установками кондиционирования воздуха. Данные установки должны иметь автоматическое управление и обеспечивать постоянный температурно-влажностный режим, определенный эксплуатационной документацией на технические средства;

системами пожарной сигнализации, автоматического газопожаротушения и противопожарной дверью;

2.10. обеспечение пожарной безопасности помещений удостоверяющего центра в соответствии с требованиями законодательства, в том числе обязательными для соблюдения требованиями технических нормативных правовых актов;

2.11. наличие персонала, обеспечивающего функционирование удостоверяющего центра, имеющего высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое образование и прошедшего переподготовку или повышение квалификации по вопросам технической и (или) криптографической защиты информации.

3. Аккредитация регистрационного центра в ГосСУОК осуществляется на соответствие следующим условиям:

3.1. присоединение регистрационного центра к политикам применения сертификатов, регламенту деятельности удостоверяющего центра, а также разработка и согласование с удостоверяющим центром регламента деятельности регистрационного центра;

3.2. использование следующих программных, программно-аппаратных и технических средств для реализации услуг и обеспечения деятельности:

3.2.1. системного и прикладного программного обеспечения. При этом:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и при необходимости другое программное обеспечение должны быть приобретены на основании лицензионного договора либо ином законном основании или быть свободно распространяемыми;

системное и прикладное программное обеспечение должно быть установлено, сконфигурировано и находиться в работоспособном состоянии;

в регистрационном центре должно использоваться только системное и прикладное программное обеспечение, которое необходимо для функционирования регистрационного центра;

3.2.2. технических средств обеспечения функционирования регистрационного центра. При этом такие технические средства должны быть исправны, корректно сконфигурированы и включать:

электронные вычислительные машины рабочих мест сотрудников;

устройства печати на бумажных носителях и их сканирования (принтеры, сканеры, многофункциональные устройства);

устройства подтверждения подлинности документов, удостоверяющих личность;

телекоммуникационное оборудование;

средства обеспечения бесперебойной работы.

Технические средства могут включать серверное оборудование.

Технические средства должны обеспечивать производительность (скорость выполнения операций), достаточную для выполнения любой прикладной задачи (услуги регистрационного центра), а также непрерывную и бесперебойную работу в ходе выполнения этой прикладной задачи.

Программные, программно-аппаратные и технические средства должны быть протестированы на предмет корректного взаимодействия с удостоверяющим центром;

3.3. наличие системы защиты информации информационной системы регистрационного центра, аттестованной в установленном порядке. При этом:

используемые средства защиты информации должны иметь сертификат соответствия или экспертное заключение;

для защиты личных ключей регистраторов регистрационного центра должны использоваться программно-аппаратные СКЗИ;

управление активами регистрационного центра посредством внешних информационных потоков должно осуществляться с использованием защищенных каналов передачи данных, обеспечивающих взаимную аутентификацию сторон;

взаимодействие информационной системы регистрационного центра с информационной системой удостоверяющего центра должно осуществляться с использованием защищенных каналов передачи данных;

должна быть обеспечена многофакторная аутентификация с использованием аппаратных носителей ключевой информации для всех учетных записей регистрационного центра, которые позволяют инициировать процедуру издания или отзыва сертификатов открытых ключей, атрибутивных сертификатов;

события технических средств, связанные с функционированием регистрационного центра, должны регистрироваться таким образом, чтобы они не были несанкционированно удалены (за исключением случаев надежного переноса на долговременные носители информации), и подлежать архивному хранению;

регистрационным центром должен обеспечиваться сбор событий, связанных с выработкой личных и открытых ключей, подтверждением подлинности документов, удостоверяющих личность, полученных в процессе издания сертификатов открытых ключей, атрибутивных сертификатов, которые передаются в удостоверяющий центр на хранение в течение не менее семи лет после того, как названные сертификаты стали недействительными;

3.4. соответствие требованиям по обеспечению безопасности при монтаже, наладке, эксплуатации и обслуживании технических средств регистрационного центра документации на соответствующее оборудование;

3.5. размещение технических средств обеспечения функционирования регистрационного центра в отдельном помещении. При этом должны обеспечиваться разграничение и контроль физического доступа к ним только уполномоченных лиц. В случае невозможности выделения такого помещения должны обеспечиваться контроль физического доступа к техническим средствам и защита этих средств от несанкционированного изменения конфигурации. В таких случаях должно быть предусмотрено применение программных, программно-аппаратных средств защиты от несанкционированного доступа или использование печатей, пломб и иных подобных элементов, позволяющих обнаружить несанкционированный доступ, а также хранение электронных вычислительных машин

и телекоммуникационного оборудования в опечатываемых и запирающихся на замок сейфах, шкафах и т.п.;

3.6. выполнение требований, определенных в подпункте 3.5 настоящего пункта, для использования технических средств обеспечения функционирования регистрационного центра в случае выезда к пользователю. При этом контроль доступа (в том числе физического) к техническим средствам должен быть обеспечен на уровне не ниже, чем в местах их постоянного хранения;

3.7. выполнение следующих требований по физическому доступу к активам регистрационного центра:

физический доступ к активам должен быть предоставлен только уполномоченным лицам и обеспечен системой контроля и управления доступом, осуществляющей проверку разрешения на доступ, либо другим способом, позволяющим проводить такую проверку;

рабочие помещения, как правило, должны быть оборудованы системой видеонаблюдения;

охрана объекта, в котором размещены технические средства, должна обеспечивать обнаружение и реагирование на несанкционированный доступ в помещения (установка средств оповещения о несанкционированном доступе, охрана помещений уполномоченной организацией (работником), при этом должен быть определен и утвержден порядок охраны помещений и реагирования ответственных лиц на несанкционированный доступ);

3.8. выполнение следующих требований по электроснабжению:

технические средства регистрационного центра в повседневном режиме использования должны быть подключены к электрической сети энергоснабжающей организации;

используемые электрические сети и электрооборудование должны соответствовать требованиям законодательства, в том числе обязательным для соблюдения требованиям технических нормативных правовых актов;

технические средства, включая телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение времени, достаточного для выполнения любой прикладной задачи (услуги регистрационного центра);

3.9. обеспечение пожарной безопасности помещений регистрационного центра в соответствии с требованиями законодательства, в том числе обязательными для соблюдения требованиями технических нормативных правовых актов;

3.10. наличие персонала, обеспечивающего оказание услуг регистрационным центром по распространению открытых ключей, прошедшего инструктаж в удостоверяющем центре.

Приложение 2

к Инструкции о порядке проведения аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

ЗАЯВЛЕНИЕ*
на проведение аккредитации в Государственной системе управления открытыми
ключами проверки электронной цифровой подписи Республики Беларусь

(наименование заявителя, регистрационный номер в Едином государственном регистре юридических

лиц и индивидуальных предпринимателей или учетный номер плательщика, место нахождения

юридического лица (заявителя), банковские реквизиты, структурное подразделение,
которое будет осуществлять функции поставщика услуг)

просит провести аккредитацию в качестве удостоверяющего и (или) регистрационного центра
в Государственной системе управления открытыми ключами проверки электронной цифровой
подписи Республики Беларусь, расположенного по адресу:

(место расположения удостоверяющего

и (или) регистрационного центра (адрес места оказания услуг и количество рабочих мест)

В качестве удостоверяющего центра выступает** _____

(наименование

удостоверяющего центра)

Обязуемся присоединиться к политике (политикам) применения сертификатов
и регламенту деятельности удостоверяющего центра.**

Выражаем согласие заключить договор на проведение аккредитации и оплатить
стоимость работ, связанных с ее проведением.

Приложение:

Руководитель организации

(подпись)

(инициалы, фамилия)

_____.____.20____

* При наступлении обстоятельств, указанных в части первой пункта 18 Инструкции о порядке проведения
аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой
подписи Республики Беларусь, аккредитованным поставщиком услуг указывается в заявлении соответствующая
информация.

** Заполняется в случае аккредитации в качестве регистрационного центра.

Приложение 3
к Инструкции о порядке проведения
аккредитации в Государственной
системе управления открытыми ключами
проверки электронной цифровой
подписи Республики Беларусь

ПЕРЕЧЕНЬ
документов (сведений), представляемых заявителем

1. Копии учредительного документа, положения о структурном подразделении, которое будет выполнять функции поставщика услуг (с указанием функций поставщика услуг в таком положении). В случае отсутствия структурного подразделения, выполняющего функции поставщика услуг, такие функции должны быть указаны в иных локальных правовых актах заявителя.

2. Для аккредитации в качестве удостоверяющего центра, кроме документов, перечисленных в пункте 1 настоящего приложения, заявитель представляет:

сведения о сертификатах соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 (далее – сертификат соответствия), или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – экспертное заключение), в отношении средств защиты информации, используемых в удостоверяющем центре;

копию аттестата соответствия системы защиты информации информационной системы удостоверяющего центра требованиям по защите информации, а также копию технического задания на создание системы защиты информации данной информационной системы либо сведения о представлении указанных документов в орган по аккредитации;

копии структурной и логической схем информационной системы удостоверяющего центра;

копию регламента деятельности удостоверяющего центра;

документы, взаимосвязанные с политикой (политиками) применения сертификатов и регламентом деятельности удостоверяющего центра, либо их копии (при наличии);

документы, содержащие информацию об инфраструктуре удостоверяющего центра (сведения о находящихся в собственности или на ином законном основании зданиях (помещениях), перечне оборудования, технических средствах и другое);

документы, подтверждающие компетентность персонала (список сотрудников, копии документов (либо сведения) о высшем образовании в области защиты информации либо высшем, или среднем специальном, или профессионально-техническом образовании и переподготовке или повышении квалификации по вопросам технической и (или) криптографической защиты информации);

документы (сведения), содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения удостоверяющего центра, обеспечении гарантированным непрерывным электроснабжением технических средств удостоверяющего центра.

3. Для аккредитации в качестве регистрационного центра, кроме документов, перечисленных в пункте 1 настоящего приложения, заявитель представляет:

копию регламента деятельности регистрационного центра, согласованного с удостоверяющим центром;

сведения о сертификатах соответствия или экспертном заключении в отношении средств защиты информации, используемых в регистрационном центре;

копию аттестата соответствия системы защиты информации информационной системы регистрационного центра требованиям по защите информации, копию технического задания на создание системы защиты информации данной информационной системы либо сведения о представлении указанных документов в орган по аккредитации;

копии структурной и логической схем информационной системы регистрационного центра;

документы (акты или протоколы тестирования, утвержденные руководителем заявителя или его уполномоченным представителем и согласованные с удостоверяющим центром) либо их копии, подтверждающие положительные результаты тестирования программных, программно-аппаратных и технических средств регистрационного центра на предмет их корректного взаимодействия с удостоверяющим центром. В таких документах указываются цель тестирования, состав участников, условия и место проведения тестирования, состав программных, программно-аппаратных и технических средств, а также результаты тестирования и другие необходимые сведения;

документы, взаимосвязанные с политикой (политиками) применения сертификатов удостоверяющего центра, к которой (которым) присоединяется регистрационный центр, и с регламентом деятельности регистрационного центра, либо их копии (при наличии);

документы, содержащие информацию об инфраструктуре регистрационного центра (сведения о находящихся в собственности или ином законном основании зданиях (помещениях), перечне оборудования, технических средствах и другое);

документы (сведения), подтверждающие прохождение персоналом инструктажа в удостоверяющем центре;

документы (сведения), содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения регистрационного центра, обеспечении гарантированным непрерывным электроснабжением технических средств регистрационного центра.

Приложение 4

к Инструкции о порядке проведения
аккредитации в Государственной
системе управления открытыми ключами
проверки электронной цифровой
подписи Республики Беларусь

Форма

ГОСУДАРСТВЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ ПРОВЕРКИ
ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ РЕСПУБЛИКИ БЕЛАРУСЬ

Оперативно-аналитический центр при Президенте Республики Беларусь
220030, г. Минск, ул. Кирова, 49

АТТЕСТАТ АККРЕДИТАЦИИ
CERTIFICATE OF ACCREDITATION

Зарегистрирован в органе по аккредитации № _____

Дата регистрации ____ 20__ г.

Действителен до ____ 20__ г.

Настоящий аттестат аккредитации подтверждает, что _____
(наименование)

и место нахождения юридического лица, которому выдан аттестат аккредитации)
аккредитовано в качестве _____

(удостоверяющего и (или) регистрационного центра)

в Государственной системе управления открытыми ключами проверки электронной цифровой
подписи Республики Беларусь.

Руководитель
органа по аккредитации
(уполномоченное лицо)

(подпись)

М.П.

(инициалы, фамилия)