

ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ
РЕСПУБЛИКИ БЕЛАРУСЬ
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

Изменения и дополнения:

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2015 г. № 48 (зарегистрировано в Национальном реестре - № 7/3106 от 12.05.2015 г.) <Т61503106>

В соответствии с пунктом 3 Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Инструкцию 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.

2. Настоящий приказ вступает в силу с 2 декабря 2013 г.

Начальник

С.В.Шпегун

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
29.11.2013 № 89

ИНСТРУКЦИЯ

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

**ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ**

1. В настоящей Инструкции, разработанной 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), определяется порядок аккредитации поставщиков услуг (далее, если не установлено иное, – заявитель) в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) и осуществления контроля за соблюдением ее условий.

2. Для целей настоящей Инструкции применяются термины и их определения в значениях, установленных Законом Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552), Законом Республики Беларусь от 28 декабря 2009 года «Об электронном документе и электронной цифровой подписи» (Национальный реестр правовых актов Республики Беларусь, 2010 г., № 15, 2/1665), техническими нормативными правовыми актами в сфере защиты информации, а также следующие термины и их определения:

аккредитация – комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие заявителя условиям аккредитации в ГосСУОК;

поставщик услуг – организация, оказывающая услуги по распространению открытых ключей проверки электронной цифровой подписи и выполняющая одну или несколько из следующих функций: достоверное подтверждение принадлежности открытого ключа определенной организации или физическому лицу, издание, распространение, хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

удостоверяющий центр (далее – УЦ) – поставщик услуг издания, распространения, хранения сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

регистрационный центр (далее – РЦ) – поставщик услуг достоверного подтверждения принадлежности открытого ключа определенной организации или физическому лицу;

реестр аккредитованных поставщиков услуг – совокупность данных о действующих поставщиках услуг, прошедших аккредитацию в ГосСУОК.

3. Аккредитация поставщиков услуг в ГосСУОК (далее – аккредитация) проводится Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – орган по аккредитации) по инициативе заявителя на соответствие условиям аккредитации по перечню согласно приложению 1 к настоящей Инструкции.

4. При проведении аккредитации заявитель и орган по аккредитации несут ответственность за соблюдение конфиденциальности полученной информации в соответствии с законодательством.

5. Аккредитация проводится на основании договора, который заключается между заявителем и органом по аккредитации.

6. Орган по аккредитации ведет реестр аккредитованных поставщиков услуг в ГосСУОК, обеспечивает открытый доступ к актуальной информации о выданных аттестатах аккредитации, текущем статусе аккредитации поставщика услуг посредством размещения соответствующей информации на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет.

7. Аккредитация включает следующие этапы:

подача заявки на аккредитацию с прилагаемыми документами и их регистрация;

анализ заявки и прилагаемых к ней документов;

принятие решения по заявке;

заключение договора между органом по аккредитации и заявителем на проведение аккредитации;

оценка заявителя на соответствие условиям аккредитации;

анализ данных, полученных после проведения оценки заявителя, и принятие решения об аккредитации;

оформление, регистрация и выдача аттестата аккредитации.

Каждый последующий этап аккредитации реализуется при положительных результатах предыдущего этапа.

8. Допускается оформление аттестата аккредитации на иностранном языке. При этом заявитель должен представить в орган по аккредитации реквизиты, подлежащие включению в аттестат аккредитации, на запрашиваемом иностранном языке.

ГЛАВА 2

ПОДАЧА ЗАЯВКИ И ПРИНЯТИЕ РЕШЕНИЯ О ПРОВЕДЕНИИ АККРЕДИТАЦИИ

9. Для проведения аккредитации заявитель направляет в орган по аккредитации заявку по форме согласно приложению 2 к настоящей Инструкции. При аккредитации в качестве регистрационного центра заявитель дополнительно указывает в заявке удостоверяющий центр и политику применения сертификатов, к которой он присоединяется.

К заявке прилагаются документы и (или) сведения согласно приложению 3 к настоящей Инструкции.

Прилагаемые к заявке документы, в том числе их копии, должны быть заверены подписью и печатью заявителя.

Указанные в части второй настоящего пункта документы представляются на языке оригинала вместе с их переводом на один из государственных языков Республики Беларусь.

10. Орган по аккредитации в месячный срок после регистрации заявки проводит анализ заявки и прилагаемых к ней документов, в том числе проверку правильности ее заполнения и достаточности представленных документов.

11. При отрицательных результатах анализа заявки заявителю сообщается о необходимости предоставления дополнительной информации или об отказе в принятии заявки.

12. Отказ в принятии заявки не препятствует повторному обращению с ней после устранения недостатков, явившихся причиной отказа.

13. При соответствии заявки установленной форме и достаточности представленных документов заявителю направляется решение о проведении аккредитации по форме согласно приложению 4 к настоящей Инструкции, а также проект договора на проведение аккредитации.

ГЛАВА 3

ОЦЕНКА ЗАЯВИТЕЛЯ НА СООТВЕТСТВИЕ УСЛОВИЯМ АККРЕДИТАЦИИ

14. Для проведения оценки заявителя на соответствие условиям аккредитации решением руководителя органа по аккредитации назначается экспертная группа, состоящая из сотрудников органа по аккредитации и республиканского унитарного предприятия «Национальный центр электронных услуг», а также при необходимости технических экспертов, привлекаемых в установленном порядке.

15. Проведение оценки заявителя включает:

оценку с выездом на место нахождения заявителя в соответствии с пунктом 16 настоящей Инструкции;

обобщение данных, полученных после оценки, и подготовку отчета в соответствии с пунктом 18 настоящей Инструкции.

16. В рамках осуществления оценки с выездом на место нахождения заявителя экспертной группой изучается:

инфраструктура, необходимая для оказания услуг по распространению открытых ключей;

наличие и состояние служебных помещений, программно-аппаратных средств электронной цифровой подписи, технических средств, используемых для функционирования программного комплекса УЦ и (или) РЦ, персональных компьютеров, локальных компьютерных сетей, программных продуктов, электронных баз данных, множительной и копировальной техники;

наличие коммуникаций, связи, системы контроля физического доступа к компонентам УЦ и (или) РЦ и системы контроля доступа к программным компонентам УЦ и (или) РЦ, системы видеонаблюдения серверных и служебных помещений УЦ и (или) РЦ, источников бесперебойного питания и резервного электропитания, установок кондиционирования воздуха в серверном помещении УЦ, систем пожарной сигнализации, автоматического

газопожаротушения, газоудаления в соответствии с условиями аккредитации по перечню согласно приложению 1 к настоящей Инструкции.

17. Экспертная группа оценивает:

возможности заявителя по оказанию услуг по распространению открытых ключей; соблюдение требований политики применения сертификатов и регламента.

Оценка проводится посредством:

наблюдения за действиями заявителя при оказании услуг по распространению открытых ключей;

моделирования процесса оказания услуг по распространению открытых ключей (выработка, хранение, резервное копирование и восстановление личного ключа подписи УЦ; регистрация пользователя; издание сертификатов открытых ключей и списков отозванных сертификатов; отзыв, приостановка, возобновление действия сертификатов открытых ключей).

18. Экспертная группа на основании объективных данных, собранных в ходе оценки, оформляет отчет и направляет его заявителю не позднее 15 дней после завершения оценки. В случае наличия несоответствий заявителя требованиям политики применения сертификатов и регламента в отчете указывается информация о необходимости проведения дополнительной оценки в целях проверки их устранения.

Отчет об оценке подписывается экспертами группы и уполномоченным представителем заявителя, который вправе высказать особое мнение о результатах работы экспертной группы, которое отражается в отчете об оценке.

19. Заявитель в установленные в отчете об оценке сроки разрабатывает корректирующие мероприятия по устранению выявленных несоответствий и представляет их руководителю экспертной группы для согласования. Срок выполнения корректирующих действий не должен превышать 90 дней с даты их согласования.

Заявитель представляет в орган по аккредитации отчет о реализации запланированных корректирующих мероприятий по устранению выявленных несоответствий.

20. Экспертная группа анализирует результаты предпринятых заявителем мероприятий на предмет их достаточности и результативности. В случае недостаточности корректирующих мероприятий экспертная группа вправе запросить дополнительную информацию. Органом по аккредитации может быть принято решение о проведении дополнительной оценки в целях контроля устранения выявленных несоответствий.

В случае непредставления необходимой информации о реализации запланированных корректирующих мероприятий в установленный срок руководитель экспертной группы информирует орган по аккредитации о целесообразности прекращения работ по аккредитации.

По результатам представления заявителем данных, свидетельствующих о выполнении корректирующих мероприятий, руководитель экспертной группы оформляет заключительный отчет об оценке заявителя. Для принятия решения об аккредитации заявителя руководитель экспертной группы представляет результаты оценки заявителя в орган по аккредитации.

21. Решение о предоставлении аккредитации, подтверждении и продлении аккредитации, приостановлении, отказе в аккредитации принимается органом по аккредитации посредством утверждения руководителем органа по аккредитации или его уполномоченным заместителем заключительного отчета по результатам оценки заявителя.

22. Основанием для приостановления аккредитации, отказа в аккредитации и отрицательного решения по аккредитации является:

неподтверждение в ходе проведения оценки заявителя его соответствия условиям аккредитации;

несоответствие деятельности аккредитованного поставщика услуг требованиям политики применения сертификатов и регламента (отказ в аккредитации или приостановление аккредитации возможно при однократном несоответствии требованиям

политики применения сертификатов и регламента, которое может повлиять на объективность и компетентность при выполнении работ);

неустранение в согласованные сроки выявленных несоответствий;

наличие отрицательных результатов оценки аккредитованного поставщика услуг, полученных при проведении его периодического контроля;

полное отсутствие деятельности аккредитованного поставщика услуг в течение более двух лет со дня принятия решения о выдаче аттестата аккредитации;

несоблюдение условий соглашения с аккредитованным поставщиком услуг в части обязательств аккредитованного поставщика услуг.

ГЛАВА 4

ОЦЕНКА АККРЕДИТОВАННОГО ПОСТАВЩИКА УСЛУГ В ЦЕЛЯХ ПОДТВЕРЖДЕНИЯ И ПРОДЛЕНИЯ АККРЕДИТАЦИИ

23. Подтверждение и продление аттестата аккредитации осуществляются по заявке аккредитованного поставщика услуг. Проведение данных работ осуществляется в порядке, предусмотренном в главе 3 настоящей Инструкции.

24. Заявка на проведение работ в целях подтверждения и продления аттестата аккредитации подается аккредитованным поставщиком услуг не позднее чем за три месяца до окончания срока действия аттестата аккредитации по форме согласно приложению 2 к настоящей Инструкции.

25. При проведении оценки аккредитованного поставщика услуг в целях подтверждения и продления аккредитации экспертной группой применяются методы, направленные на выявление объективных свидетельств выполнения требований политики применения сертификатов и регламента при оказании услуг по распространению открытых ключей за предыдущий период действия аттестата аккредитации по результатам деятельности аккредитованного поставщика услуг.

При этом экспертная группа также оценивает:

выполнение аккредитованным поставщиком услуг условий постаккредитационного соглашения;

выполнение мероприятий по результатам предыдущих оценок (периодического контроля), проведенных органом по аккредитации;

результаты анализа информации, поступившей от республиканских органов государственного управления;

результаты анализа обратной связи с клиентами аккредитованного поставщика услуг (результаты рассмотрения отзывов, опросов, обращений).

26. При принятии органом по аккредитации положительного решения о продлении аккредитованному поставщику услуг срока действия аттестата аккредитации последнему присваивается тот же регистрационный номер на новый срок действия аттестата аккредитации.

27. Орган по аккредитации заключает соглашение с аккредитованным поставщиком услуг на новый срок действия аттестата аккредитации.

28. Информация о продлении срока действия аттестата аккредитации вносится в реестр не позднее 15 дней после принятия решения об аккредитации.

ГЛАВА 5

ПОРЯДОК ВЫДАЧИ, ПРОДЛЕНИЕ СРОКА ДЕЙСТВИЯ, ПРИОСТАНОВЛЕНИЕ, ПРЕКРАЩЕНИЕ, ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ АТТЕСТАТА АККРЕДИТАЦИИ

29. Выдача, продление срока действия, приостановление, прекращение, возобновление действия аттестата аккредитации осуществляются по результатам проведенной оценки заявителя (аккредитованного поставщика услуг) органом по аккредитации.

30. При положительном принятии решения об аккредитации орган по аккредитации в течение 15 рабочих дней со дня принятия такого решения выдает заявителю аттестат аккредитации по форме согласно приложению 5 к настоящей Инструкции.

31. Аттестат аккредитации выдается сроком на 5 лет.

32. Внесение изменений и (или) дополнений в аттестат аккредитации осуществляется одним из следующих способов:

изложением аттестата аккредитации в новой редакции (при изменении наименования аккредитованного поставщика услуг и (или) его структурного подразделения, их местонахождения);

проставлением отметки о внесении изменений и (или) дополнений, продлении срока действия, приостановлении, прекращении, возобновлении действия аттестата аккредитации на оборотной стороне бланка аттестата аккредитации.

33. При наличии у одного поставщика услуг нескольких обособленных структурных подразделений, оказывающих услуги по распространению открытых ключей, аттестату аккредитации присваивается один регистрационный номер, на оборотной стороне бланка аттестата аккредитации приводится перечень аккредитованных поставщиков услуг.

34. В случае продления действия аттестата аккредитации на время проведения работ по подтверждению и продлению действия аккредитации на оборотной стороне бланка аттестата аккредитации проставляется отметка о сроке продления.

35. Аттестат аккредитации, а также отметки о продлении срока действия, приостановлении, прекращении, возобновлении, внесении изменений и (или) дополнений подписываются руководителем органа по аккредитации или его уполномоченным заместителем и скрепляются гербовой печатью органа по аккредитации.

36. Аттестат аккредитации выдается руководителю аккредитованного поставщика услуг или его уполномоченному представителю, который расписывается о его получении в журнале регистрации аттестатов аккредитации.

37. Одновременно с выдачей аттестата аккредитации заключается соглашение органа по аккредитации с аккредитованным поставщиком услуг по форме согласно приложению 6 к настоящей Инструкции.

38. В органе по аккредитации хранятся копии выданных аттестатов аккредитации, заверенные в установленном порядке.

39. Информация о выдаче аттестата аккредитации по истечении срока его действия, при прекращении, приостановлении, возобновлении, продлении действия аккредитации, внесенных изменениях и (или) дополнениях в аттестат аккредитации вносится в реестр аккредитованных поставщиков услуг ГосСУОК.

40. Аккредитованный поставщик услуг обязан представить аттестат аккредитации в орган по аккредитации для внесения изменений и (или) дополнений не позднее 15 дней после получения выписки из протокола органа по аккредитации о принятом в отношении его решении. В случае непредставления аккредитованным поставщиком услуг в установленный срок аттестата аккредитации органом по аккредитации составляется акт с указанием причин непредставления.

ГЛАВА 6

КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ УСЛОВИЙ АККРЕДИТАЦИИ

41. С даты принятия решения о выдаче аттестата аккредитации орган по аккредитации осуществляет контроль за деятельностью аккредитованного поставщика услуг в форме проверок, проводимых в соответствии с планом проверок, размещаемым на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет не позднее 20 декабря года, предшествующего году проведения проверки.

Без включения в план, указанный в части первой настоящего пункта, проверки аккредитованных поставщиков услуг могут назначаться руководителем органа по аккредитации при наличии сведений, в том числе полученных от государственного органа,

иной организации или физического лица, свидетельствующих о совершаемом (совершенном) нарушении требований политики применения сертификатов и (или) регламента аккредитованного поставщика услуг, а также условий аккредитации и постаккредитационного соглашения.

42. Для проведения проверки решением руководителя органа по аккредитации назначается комиссия и определяется ее председатель.

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

44. Проверка аккредитованного поставщика услуг проводится в соответствии с порядком, установленным в главе 3 настоящей Инструкции. При проведении проверки председатель комиссии самостоятельно определяет методы и способы ее осуществления.

45. По результатам проверки оформляется отчет об оценке, в котором дается оценка состояния деятельности аккредитованного поставщика услуг, приводятся соответствующие выводы о соблюдении им политики применения сертификатов и регламента.

46. Один экземпляр отчета по результатам проверки, подписанный председателем комиссии, передается аккредитованному поставщику услуг.

47. Несоответствия, отмеченные в отчете, должны быть устранены аккредитованным поставщиком услуг в сроки, согласованные с председателем комиссии.

48. Аккредитованный поставщик услуг должен представить в орган по аккредитации отчет о выполнении запланированных корректирующих мероприятий.

49. Неустранение в согласованные сроки выявленных несоответствий является основанием для приостановления аккредитации в ГосСУОК.

Приложение 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 редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.04.2015 № 48)

ПЕРЕЧЕНЬ

условий, на соответствие которым осуществляется аккредитация поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

1. Поставщик услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) должен иметь специальное разрешение (лицензию) на осуществление деятельности по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг по распространению открытых ключей проверки подписи.

2. Аккредитация удостоверяющего центра (далее – УЦ) в ГосСУОК осуществляется на соответствие следующим условиям:

2.1. УЦ должен разработать политику применения сертификатов УЦ и регламент УЦ в соответствии с требованиями СТБ 34.101.48-2012 «Информационные технологии и

безопасность. Требования к политике применения сертификатов удостоверяющих центров» и согласовать указанные документы с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ);

2.2. в УЦ должны быть реализованы требования в соответствии с СТБ 34.101.48-2012:

по управлению ключами (по выработке личного ключа подписи УЦ; хранению, резервному копированию и восстановлению личного ключа подписи УЦ; распространению открытых ключей УЦ; использованию личного ключа УЦ; действиям по окончании срока действия личного ключа УЦ; управлению средствами электронной цифровой подписи (далее – ЭЦП)), используемыми для издания сертификатов открытых ключей;

по управлению сертификатами открытых ключей (по регистрации субъектов для получения сертификата открытого ключа; изданию, возобновлению действия и обновлению данных; распространению, отзыву и приостановке действия сертификатов открытых ключей), издаваемыми УЦ;

по организационному функционированию и управлению деятельностью УЦ;

2.3. для реализации услуг УЦ и обеспечения своей деятельности поставщики услуг, кроме выполнения требований по управлению деятельностью УЦ, определенных в СТБ 34.101.48-2012, должны использовать в УЦ следующие программные и технические средства:

2.3.1. системное и прикладное программное обеспечение:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и другое программное обеспечение (при необходимости) должны быть приобретены в соответствии с законодательством (иметь соответствующие лицензии производителей или быть свободно распространяемыми);

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

2.3.2. программно-аппаратные средства ЭЦП, используемые для генерации личного ключа подписи УЦ и выработки 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/ВУ) на соответствие следующим взаимосвязанным с данным техническим регламентом государственным стандартам:

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, приложения Д и Е);

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

СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (подразделы 6.2 и 6.3 раздела б);

СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» (подраздел 5.6 раздела 5);

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 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

СТБ 34.101.60-2013 «Информационные технологии и безопасность. Алгоритмы разделения секрета» (раздел 7, таблица А1 приложения А);

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

СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)»;

СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации»;

2.3.2.2. должны быть сертифицированы на соответствие требованиям СТБ 34.101.49-2012 «Информационные технологии и безопасность. Формат карточки открытого ключа»;

2.3.2.3. для генерации случайных чисел должны использовать аппаратный датчик случайных чисел;

2.3.2.4. должны обеспечивать невозможность доступа к криптографическим ключам в случае несанкционированного вскрытия корпуса;

2.3.2.5. настройка и выполнение функций ПАС ЭЦП должны осуществляться путем подачи команд с автоматизированного рабочего места (далее – АРМ) администратора ПАС ЭЦП. Взаимодействие ПАС ЭЦП с АРМ администратора должно производиться по надежному каналу передачи данных, который логически отличается от других информационных каналов и обеспечивает гарантированную идентификацию конечных сторон, а также защиту данных от модификации и раскрытия. Средства канального (линейного) шифрования между ПАС ЭЦП и АРМ администратора должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям СТБ 34.101.65-2014;

2.3.3. средства канального (линейного) шифрования между УЦ и удаленным регистрационным центром (далее – РЦ), которые должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента ТР 2013/027/ВУ;

2.3.4. технические средства обеспечения функционирования УЦ и (или) РЦ (далее – ТС).

ТС обеспечения работы программного комплекса УЦ должны быть исправны, корректно сконфигурированы, работоспособны и включать:

сервер (серверы) УЦ;

средства резервного копирования;

сервер (устройство) получения точного времени;

телекоммуникационное оборудование;

компьютеры рабочих мест сотрудников УЦ;

устройства печати на бумажных носителях (принтеры).

При реализации УЦ услуги по регистрации субъектов должны быть дополнительно предусмотрены следующие ТС:

сервер (серверы) или АРМ РЦ;

устройства печати на бумажных носителях (принтеры);

средства обеспечения бесперебойной работы;

устройства подтверждения подлинности идентификационных документов.

ТС должны обеспечивать возможность непрерывной и бесперебойной работы программного обеспечения УЦ, а также производительность (скорость выполнения

операций), достаточную для выполнения оператором любой прикладной задачи (услуг УЦ) в течение 30 минут;

2.4. система защиты информации УЦ должна быть создана и аттестована в соответствии с законодательством и включать в себя следующие компоненты:

средства криптографической защиты информации;

средства защиты информации от несанкционированного доступа, включая ПАС аутентификации, разграничения доступа, межсетевые экраны;

средства активного аудита информационной безопасности УЦ;

средства обнаружения вторжений;

средства резервного копирования и архивирования данных;

средства обеспечения контроля целостности информации, программных и аппаратных компонентов комплекса, в том числе криптографическими методами;

средства обеспечения доступности сервисов УЦ и (или) РЦ и безотказной работы комплекса, включающие регулярно обновляемые антивирусные средства;

2.5. средства защиты информации, используемые в системе защиты информации УЦ, должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента ТР 2013/027/ВУ;

2.6. требования по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании ТС УЦ (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и т.п.) по допустимым уровням освещенности, вибрационных и шумовых нагрузок должны соответствовать техническим удостоверениям на соответствующие виды оборудования;

2.7. серверы УЦ, серверы баз данных, серверы средств резервного копирования и телекоммуникационное оборудование поставщиков услуг должны размещаться в выделенном помещении;

2.8. требования по физическому доступу к компонентам УЦ:

физический доступ к компонентам УЦ должен быть защищен как минимум двумя уровнями доступа;

на каждом уровне доступа осуществляется проверка разрешения на доступ;

контроль доступа к программным компонентам УЦ осуществляется с использованием двухфакторной аутентификации, включая использование аппаратных носителей ключевой информации;

серверное помещение и рабочие помещения УЦ должны быть оборудованы системами контроля доступа и видеонаблюдения;

здание, в котором размещены ТС УЦ, должно находиться под охраной в соответствии с Указом Президента Республики Беларусь от 25 октября 2007 г. № 534 «О мерах по совершенствованию охранной деятельности» (Национальный реестр правовых актов Республики Беларусь, 2007 г., № 262, 1/9048);

2.9. требования к электроснабжению:

ТС УЦ в повседневном режиме должны быть подключены к общегородской сети электроснабжения;

электрические сети и электрооборудование, используемые в УЦ, должны отвечать требованиям технических нормативных правовых актов (далее – ТНПА);

серверы, телекоммуникационное оборудование и ТС сотрудников УЦ должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение 30 минут после прекращения основного электроснабжения;

при исчезновении напряжения промышленной сети должно быть предусмотрено резервное электропитание ТС УЦ;

в качестве источника резервного питания может использоваться дизель-генераторная установка, подключенная к потребителям электропитания и обеспечивающая автоматическую подачу необходимого электроснабжения в течение 30 минут после

отключения общегородской сети электроснабжения (дизель-генераторная установка не требуется при наличии двух вводов в здание УЦ от различных подстанций);

2.10. серверное помещение УЦ должно быть оборудовано двумя установками кондиционирования воздуха. Установки должны управляться автоматизированной системой и обеспечивать постоянный температурно-влажностный режим, определенный эксплуатационной документацией на ТС УЦ;

2.11. серверное помещение УЦ должно быть оборудовано системами пожарной сигнализации, автоматического газопожаротушения, газоудаления и противопожарной дверью с огнестойкостью не менее одного часа;

2.12. пожарная безопасность помещений УЦ должна обеспечиваться в соответствии с нормами и требованиями ТНПА и законодательства.

3. Аккредитация РЦ в ГосСУОК осуществляется на соответствие следующим условиям:

3.1. РЦ должен присоединяться к политике применения сертификатов УЦ, согласованной с ОАЦ, и выполнять ее в части оказания услуг по регистрации субъектов УЦ;

3.2. в РЦ должны быть реализованы требования в соответствии с СТБ 34.101.48-2012 по регистрации субъектов для получения сертификатов УЦ;

3.3. для реализации услуг РЦ и обеспечения своей деятельности, кроме выполнения требований по управлению деятельностью РЦ, определенных в политике применения сертификатов УЦ, в РЦ должны использоваться следующие программные и технические средства:

3.3.1. системное и прикладное программное обеспечение:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и другое программное обеспечение (при необходимости) должны быть приобретены в соответствии с законодательством (иметь соответствующие лицензии производителей или быть свободно распространяемыми);

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

3.3.2. средства выработки и проверки ЭЦП, которые должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента ТР 2013/027/ВУ на соответствие следующим взаимосвязанным с данным техническим регламентом государственным стандартам:

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, приложения Д и Е);

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

СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (подразделы 6.2 и 6.3 раздела 6);

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 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации».

Средства выработки и проверки ЭЦП РЦ должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь на соответствие требованиям СТБ 34.101.49-2012;

3.3.3. ТС обеспечения функционирования РЦ:

3.3.3.1. ТС обеспечения работы программного комплекса РЦ должны быть исправны, корректно сконфигурированы, работоспособны и включать:

компьютеры рабочих мест сотрудников РЦ;

устройства печати на бумажных носителях (принтеры);

устройства подтверждения подлинности идентификационных документов;

телекоммуникационное оборудование;

средства обеспечения бесперебойной работы;

3.3.3.2. ТС обеспечения программного комплекса РЦ могут включать:

серверы баз данных;

серверы архивного хранения электронных документов;

3.3.3.3. ТС должны обеспечивать производительность (скорость выполнения операций), достаточную для выполнения оператором любой прикладной задачи (услуг РЦ), а также непрерывную и бесперебойную работу в ходе выполнения этой прикладной задачи;

3.3.4. программные, программно-технические и технические средства РЦ, которые должны быть протестированы на предмет взаимодействия с УЦ, в интересах которого РЦ будут оказываться услуги (акты либо протоколы тестирования);

3.4. система защиты информации РЦ должна быть создана и аттестована в соответствии с законодательством;

3.5. средства защиты информации, используемые в системе защиты информации РЦ, должны быть сертифицированы в Национальной системе подтверждения соответствия Республики Беларусь по требованиям технического регламента ТР 2013/027/ВУ;

3.6. требования по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании ТС РЦ (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и т.п.) по допустимым уровням освещенности, вибрационных и шумовых нагрузок должны соответствовать техническим удостоверениям на соответствующие виды оборудования;

3.7. компьютеры рабочих мест сотрудников РЦ и телекоммуникационное оборудование РЦ должны размещаться в выделенном помещении. В случае невозможности выделения такого размещения должна обеспечиваться защита ТС от несанкционированного изменения их конфигурации и несанкционированного доступа к интерфейсным портам этих средств (применение программных, программно-аппаратных средств защиты от несанкционированного доступа, саморазрушающихся наклеек, стикеров; хранение ТС в опечатываемых коммутационных шкафах);

3.8. требования по физическому доступу к компонентам РЦ:

физический доступ к компонентам РЦ должен быть защищен как минимум двумя уровнями доступа;

на каждом уровне доступа должна осуществляться проверка разрешения на доступ;

контроль доступа к программным компонентам РЦ должен осуществляться с использованием двухфакторной аутентификации, включая использование аппаратных носителей ключевой информации;

рабочие места РЦ по возможности должны быть оборудованы системами видеонаблюдения;

здание, в котором размещены ТС УЦ, должно находиться под охраной в соответствии с Указом Президента Республики Беларусь от 25 октября 2007 г. № 534 «О мерах по совершенствованию охранной деятельности»;

3.9. требования по электроснабжению:

ТС РЦ в повседневном режиме должны быть подключены к общегородской сети электроснабжения;

электрические сети и электрооборудование, используемые в РЦ, должны отвечать требованиям ТНПА;

после прекращения основного электроснабжения телекоммуникационное оборудование и ТС сотрудников РЦ должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение времени, достаточного для выполнения оператором любой прикладной задачи (услуги РЦ);

3.10. пожарная безопасность помещений РЦ должна обеспечиваться в соответствии с нормами и требованиями ТНПА и законодательства.

Приложение 2
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

Форма

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

(наименование заявителя, местонахождение)

просит провести аккредитацию в качестве удостоверяющего и (или) регистрационного центра в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Необходимые документы по аккредитации прилагаются.

Заявитель готов предоставить условия для проведения аккредитации и необходимые документы.

Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аккредитации.

Приложение:

Руководитель организации _____

(подпись)

_____ (инициалы, фамилия)

__ . __ . 20__

М.П.

Главный бухгалтер _____

(подпись)

_____ (инициалы, фамилия)

__ . __ . 20__

Приложение 3
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 редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.04.2015 № 48)

ПЕРЕЧЕНЬ

документов, представляемых поставщиком услуг при аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

1. Копии учредительного документа (за исключением положений, касающихся уставного фонда и порядка распределения прибыли); положения о структурном подразделении, которое будет выполнять функции поставщика услуг; свидетельства о государственной регистрации в Едином государственном регистре юридических лиц и индивидуальных предпринимателей.

2. Копия специального разрешения (лицензии) на осуществление деятельности по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг по распространению открытых ключей.

3. Заявитель при аккредитации в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – ГосСУОК) в качестве удостоверяющего центра (далее – УЦ) кроме документов, перечисленных в пунктах 1 и 2 настоящего приложения, должен представить следующие документы:

3.1. копии политики применения сертификатов и регламента УЦ заявителя, а также сертификата соответствия данных документов требованиям СТБ 34.101.48-2012 «Информационные технологии и безопасность. Требования к политике применения сертификатов удостоверяющих центров», выданного в Национальной системе подтверждения соответствия Республики Беларусь, либо протокола оценки аккредитованной лабораторией соответствия данных документов СТБ 34.101.48-2012;

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/ВУ) с взаимосвязанными с данным техническим регламентом государственными стандартами, указанными в подпункте 2.3.2.1 пункта 2 приложения 1 к настоящему приказу;

СТБ 34.101.49-2012 «Информационные технологии и безопасность. Формат карточки открытого ключа»;

3.3. копию аттестата соответствия требованиям по защите информации системы защиты информации информационной системы УЦ, выданного в соответствии с

законодательством, а также копию задания по безопасности или технического задания на данную информационную систему;

3.4. копии сертификатов соответствия, выданных в Национальной системе подтверждения соответствия Республики Беларусь, на соответствие средств защиты информации, используемых в системе защиты информации, требованиям ТР 2013/027/ВУ;

3.5. документы, взаимосвязанные с политикой применения сертификатов и регламентом УЦ (стандарты организации, документированные процедуры, рабочие инструкции), либо их копии;

3.6. документы, содержащие информацию об инфраструктуре поставщика услуг (помещения, оборудование, применяемые средства защиты и другое) и о компетентности персонала (список сотрудников, копии дипломов об окончании учебных заведений, свидетельств повышения квалификации в области защиты информации);

3.7. документы, содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения УЦ, обеспечении гарантированным непрерывным электроснабжением ТС УЦ.

4. Кроме документов, перечисленных в пунктах 1 и 2 настоящего приложения, заявитель при аккредитации в ГосСУОК в качестве регистрационного центра (далее – РЦ) должен представить следующие документы:

4.1. копию политики применения сертификатов УЦ, согласованную с Оперативно-аналитическим центром при Президенте Республики Беларусь, к которой присоединяется заявитель;

4.2. копию регламента работы РЦ заявителя;

4.3. копии сертификатов соответствия, выданных в Национальной системе подтверждения соответствия Республики Беларусь, на соответствие средств выработки и проверки ЭЦП требованиям ТР 2013/027/ВУ с взаимосвязанными с данным техническим регламентом государственными стандартами, указанными в подпункте 3.3.2 пункта 3 приложения 1 к настоящему приказу, и СТБ 34.101.49-2012;

4.4. копию аттестата соответствия требованиям по защите информации системы защиты информации информационной системы РЦ, выданного в соответствии с законодательством, а также копию задания по безопасности или технического задания на данную информационную систему;

4.5. копии сертификатов соответствия средств защиты информации, используемых в системе защиты информации РЦ, выданных в Национальной системе подтверждения соответствия Республики Беларусь, на соответствие требованиям ТР 2013/027/ВУ;

4.6. документы (акты либо протоколы тестирования, утвержденные руководителями организаций), подтверждающие положительные результаты тестирования программных, программно-технических и технических средств РЦ на предмет корректного взаимодействия с УЦ;

4.7. документы, взаимосвязанные с политикой применения сертификатов УЦ, к которой присоединяется РЦ, и с регламентом РЦ (стандарты организации, документированные процедуры, рабочие инструкции), либо их копии;

4.8. документы, содержащие информацию об инфраструктуре поставщика услуг (помещения, оборудование, применяемые средства защиты и другое) и о компетентности персонала (список сотрудников, копии дипломов об окончании учебных заведений, свидетельств повышения квалификации в области защиты информации);

4.9. документы, содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения РЦ, гарантированным непрерывным электроснабжением ТС РЦ.

Приложение 4
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 редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.04.2015 № 48)

РЕШЕНИЕ
по заявке на проведение аккредитации
от «__» _____ 20__ г. № _____

В Оперативно-аналитическом центре при Президенте Республики Беларусь рассмотрена заявка _____
(наименование заявителя)

на проведение аккредитации _____
(наименование удостоверяющего (регистрационного) центра)

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

На основании положительного решения по рассмотрению заявки сообщаем, что:

1. Аккредитация будет проведена на соответствие условиям аккредитации согласно требованиям Инструкции о порядке проведения аккредитации поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и осуществления контроля за соблюдением условий аккредитации, утвержденной приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 29 ноября 2013 г. № 89 (Национальный правовой Интернет-портал Республики Беларусь, 06.12.2013, 7/2650).

2. Оценка на соответствие условиям аккредитации будет проведена по месту нахождения заявителя _____
(область, район, город)

(улица, номер дома, номер помещения)

3. Аккредитация будет проводиться на договорной основе.

(должность)

(подпись)
М.П.

(инициалы, фамилия)

Приложение 5
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 редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.04.2015 № 48)

Форма

АТТЕСТАТ АККРЕДИТАЦИИ
CERTIFICATE OF ACCREDITATION

Регистрационный номер _____
(номер в реестре органа по аккредитации)
от _____ подтверждает, что
(дата принятия решения о предоставлении аккредитации)

(наименование аккредитованного структурного подразделения)

(местонахождение аккредитованного структурного подразделения)

(наименование юридического лица, которому выдается аттестат аккредитации)

(местонахождение юридического лица, которому выдается аттестат аккредитации)
аккредитован в качестве _____
(удостоверяющего/регистрационного центра)
в Государственной системе управления открытыми ключами проверки электронной
цифровой подписи Республики Беларусь.

Срок действия
аттестата аккредитации: с _____ по _____

(населенный пункт, в котором
произведена выдача аттестата)

(дата выдачи аттестата
аккредитации)

Руководитель
органа по аккредитации

(подпись)
М.П.

(инициалы, фамилия)

Приложение 6
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 редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
30.04.2015 № 48)

**ГОСУДАРСТВЕННАЯ СИСТЕМА
УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ
ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ
РЕСПУБЛИКИ БЕЛАРУСЬ**

**СОГЛАШЕНИЕ № ____
с аккредитованным поставщиком услуг**

Срок действия
с _____.20__ по _____.20__

Оперативно-аналитический центр при Президенте Республики Беларусь, в
дальнейшем именуемый «орган по аккредитации», в лице _____
(должность, фамилия и инициалы)

с одной стороны и _____,
(наименование заявителя)

в дальнейшем именуемый(ое) «аккредитованный поставщик услуг», в лице руководителя
_____ с другой стороны, вместе
(должность, фамилия и инициалы)

именуемые «сторонами», заключили настоящее соглашение о нижеследующем:

1. Орган по аккредитации имеет право:

1.1. проводить контроль за соблюдением условий аккредитации в форме проверок, осуществляемых в сроки, установленные планом проверок, размещаемым на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет, либо в иные сроки, при наличии сведений, свидетельствующих о совершаемом (совершенном) нарушении требований политики применения сертификатов открытых ключей и (или) регламента удостоверяющего (регистрационного) центра;

1.2. оказывать консультативную и методическую помощь аккредитованному поставщику услуг по вопросам соблюдения условий аккредитации.

2. Орган по аккредитации обязуется информировать аккредитованного поставщика услуг об изменениях требований к условиям аккредитации путем размещения информации об изменениях на официальном сайте органа по аккредитации в глобальной компьютерной сети Интернет или иным способом, установленным законодательством Республики Беларусь.

3. Аккредитованный поставщик услуг имеет право:

3.1. подавать в орган по аккредитации заявление о выдаче, продлении срока действия, приостановлении, прекращении, возобновлении действия аттестата аккредитации;

3.2. вносить на рассмотрение органа по аккредитации предложения по совершенствованию правовых актов, регулирующих создание и поддержание единого пространства доверия к сертификатам открытых ключей, а также функционирование

Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь;

3.3. принимать участие в работе экспертных комиссий по урегулированию споров, связанных с использованием электронной цифровой подписи (далее – ЭЦП);

3.4. обращаться в орган по аккредитации по вопросам урегулирования споров, связанных с применением электронных документов и ЭЦП.

4. Аккредитованный поставщик услуг обязуется:

4.1. на основании аттестата аккредитации от __. __.20__ № _____ оказывать услуги по распространению открытых ключей проверки ЭЦП в качестве удостоверяющего центра (регистрационного центра);

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 16 октября 2012 г. № 79 «О некоторых вопросах функционирования государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь» (Национальный правовой Интернет-портал Республики Беларусь, 24.10.2012, 7/2222);

4.3. осуществлять управление открытыми ключами в соответствии с политикой применения сертификатов открытых ключей, согласованной с органом по аккредитации;

4.4. обеспечивать беспрепятственный доступ на территорию аккредитованного поставщика услуг, а также физический доступ к оборудованию, используемому для изготовления и отзыва сертификатов открытых ключей, представителям органа по аккредитации, осуществляющим контроль за соблюдением условий аккредитации, и создавать им все условия, необходимые для его проведения;

4.5. оплачивать все расходы, связанные с осуществлением контроля за соблюдением условий аккредитации;

4.6. информировать орган по аккредитации:

незамедлительно – в случае компрометации личного ключа удостоверяющего центра (регистратора);

в течение суток – о случаях возникновения нештатных ситуаций или об изменении условий эксплуатации удостоверяющего (регистрационного) центра;

не позднее чем за трое суток – о планируемых изменениях условий эксплуатации удостоверяющего (регистрационного) центра;

4.7. вести учет нарушений порядка оказания услуг подписчикам (субъектам), с которыми заключены гражданско-правовые договоры, и информировать о них орган по аккредитации в течение пяти рабочих дней с момента их возникновения.

5. За неисполнение или ненадлежащее исполнение условий аккредитации аккредитованный поставщик услуг несет ответственность в порядке и размере, определяемых законодательством Республики Беларусь.

6. Во всем, что не урегулировано настоящим соглашением, стороны руководствуются законодательством Республики Беларусь.

7. Настоящее соглашение составлено в двух экземплярах, один из которых находится в органе по аккредитации, другой – у аккредитованного поставщика услуг.

8. Соглашение вступает в силу с момента его подписания обеими сторонами.

Руководитель
органа по аккредитации

Руководитель аккредитованного
поставщика услуг

(подпись)
__ . __ .20__
М.П.

(инициалы, фамилия)

(подпись)
__ . __ .20__
М.П.

(инициалы, фамилия)