АППАРАТ ГУБЕРНАТОРА ИРКУТСКОЙ ОБЛАСТИ И
ПРАВИТЕЛЬСТВА ИРКУТСКОЙ ОБЛАСТИ

П Р И К А З

30 марта 2017 года № 20-пра

Иркутск

Об установлении Порядка реализации функций удостоверяющего центра аппарата Губернатора Иркутской области и Правительства Иркутской области и исполнения его обязанностей

В целях организации деятельности удостоверяющего центра аппарата Губернатора Иркутской области и Правительства Иркутской области, в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», руководствуясь статьей 21 Устава Иркутской области

П Р И К А З Ы В А Ю:

1. Установить Порядок реализации функций удостоверяющего центра аппарата Губернатора Иркутской области и Правительства Иркутской области и исполнения его обязанностей (прилагается).

2. Настоящий приказ подлежит официальному опубликованию в общественно-политической газете «Областная».

3. Настоящий приказ вступает в силу с момента аккредитации удостоверяющего центра аппарата Губернатора Иркутской области и Правительства Иркутской области в соответствии с законодательством.

Заместитель Губернатора Иркутской области – руководитель аппарата Губернатора Иркутской области и Правительства Иркутской области Д.В. Чернышов

УСТАНОВЛЕН
приказом аппарата Губернатора Иркутской области и Правительства Иркутской области
от 30 марта 2017 года № 20-пра

ПОРЯДОК РЕАЛИЗАЦИИ ФУНКЦИЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АППАРАТА ГУБЕРНАТОРА ИРКУТСКОЙ ОБЛАСТИ И ПРАВИТЕЛЬСТВА ИРКУТСКОЙ ОБЛАСТИ И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ

Раздел I. ОБЩИЕ ПОЛОЖЕНИЯ

Глава 1. ПРЕДМЕТ РЕГУЛИРОВАНИЯ ПОРЯДКА

1. Удостоверяющий центр аппарата Губернатора Иркутской области и Правительства Иркутской области (далее – УЦ) является удостоверяющим центром в области создания и выдачи сертификатов ключей проверки электронных подписей для электронного взаимодействия исполнительных органов государственной власти Иркутской области, государственных учреждений Иркутской области, органов местного самоуправления муниципальных образований Иркутской области, участвующих в обмене электронными документами с исполнительными органами государственной власти Иркутской области, государственными учреждениями Иркутской области, органами местного самоуправления муниципальных образований Иркутской области (далее – органы, учреждения).

Настоящий Порядок определяет условия и порядок создания и выдачи сертификатов ключей проверки электронных подписей.

УЦ осуществляет свою деятельность в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ), приказами Федеральной службы безопасности Российской Федерации, другими нормативными правовыми актами.

2. В соответствии с настоящим Порядком обеспечивается создание и выдача ключей электронной подписи и сертификатов ключей проверки электронной подписи для лиц, замещающих государственные должности Иркутской области, государственных гражданских служащих Иркутской области, работников государственных учреждений Иркутской области, лиц, замещающих муниципальные должности, муниципальных служащих, действующих от своего имени или от имени органов, учреждений при обмене электронными документами (далее – сотрудники органов, учреждений).

Действие настоящего Порядка распространяется на сотрудников органов, учреждений, обращающихся в УЦ с заявлением на создание сертификата ключа проверки электронной подписи.

С момента подачи указанного заявления до момента прекращения действия сертификата ключа проверки электронной подписи сотрудники органов, учреждений исполняют обязанности, предусмотренные настоящим Порядком.

3. Деятельность УЦ осуществляется на безвозмездной основе.

4. В настоящем Порядке используются термины, применяемые в следующих значениях:

администратор УЦ – сотрудник отдела технической защиты информации Губернатора Иркутской области и Правительства Иркутской области, уполномоченный на совершение действий в соответствии с настоящим Порядком;

помощник администратора – сотрудник отдела технической защиты информации Губернатора Иркутской области и Правительства Иркутской области, уполномоченный на совершение действий в соответствии с настоящим Порядком, в том числе в отсутствие администратора УЦ;

ключевой носитель – отчуждаемый физический носитель (flash-накопитель), на котором содержится ключ электронной подписи или может содержаться ключ электронной подписи;

ключевые файлы – файлы, содержащие закрытый ключ электронной подписи, открытый ключ электронной подписи, квалифицированный сертификат ключа проверки электронной подписи, иную вспомогательную техническую информацию;

файл запроса на создание сертификата ключа проверки электронной подписи – файл, автоматически генерируемый при создании ключа электронной подписи, содержащий информацию, аналогичную информации, указанной в заявлении на создание сертификата ключа проверки электронной подписи, и предоставляемый в УЦ одновременно с указанным заявлением.

5. Срок действия ключевых файлов составляет один год.

6. Начало периода действия ключевых файлов владельца сертификата ключа проверки электронной подписи исчисляется с даты и времени его генерации.

7. Хранение сертификатов ключей проверки электронных подписей в УЦ осуществляется на протяжении всего времени существования УЦ.

Глава 2. СВЕДЕНИЯ ОБ УЦ

8. Подразделением аппарата Губернатора Иркутской области и Правительства Иркутской области (далее – Аппарат), обеспечивающим функционирование УЦ, является отдел технической защиты информации Губернатора Иркутской области и Правительства Иркутской области (далее – Отдел).

9. Информация об УЦ:

1) место нахождения: г. Иркутск, ул. Ленина, 1А, кабинет № 160/4;

2) телефон: (3952) 25-64-16, 25-64-86;

3) почтовый адрес для направления документов и обращений: 664027, г. Иркутск, ул. Ленина, дом 1А;

4) официальный сайт: http://inform.irkobl.ru;
5) адрес электронной почты: uc@govirk.ru.
10. График работы УЦ:
понедельник 9-00 – 12-00, 14-00 – 16-00;
вторник 9-00 – 12-00, 14-00 – 16-00;
среда 9-00 – 12-00, 14-00 – 16-00;
четверг 9-00 – 12-00, 14-00 – 16-00;
пятница 9-00 – 12-00, 14-00 – 16-00;
суббота, воскресенье – выходные дни.

Глава 3. ПОРЯДОК ИНФОРМИРОВАНИЯ О ПРЕДОСТАВЛЕНИИ УСЛУГ УЦ

11. Для получения информации о порядке создания и выдачи сертификатов ключей проверки электронных подписей заинтересованные лица обращаются в УЦ.

12. Информация предоставляется:

1) при личном обращении в УЦ;

2) с использованием средств телефонной, электронной связи в соответствии с пунктом 9 настоящего Порядка, в том числе через официальный сайт Отдела в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») по адресу: http://irkobl.ru/sites/inform;

3) письменно в случае письменного обращения по адресу, указанному в пункте 9 настоящего Порядка.

Порядок рассмотрения отдельных обращений граждан осуществляется в соответствии с Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Раздел II. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УЦ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

Глава 4. ОКАЗЫВАЕМЫЕ УЦ УСЛУГИ

13. Целью деятельности УЦ является обеспечение участия в электронном взаимодействии сотрудников органов, учреждений.

14. Задачей УЦ является оказание услуг по созданию и выдаче сертификатов ключей проверки электронных подписей (далее – услуги) сотрудникам органов, учреждений, имеющим намерение на получение сертификата ключа проверки электронной подписи с целью осуществления электронного документооборота (далее – заявители).

Глава 5. ФУНКЦИИ УЦ

15. УЦ в соответствии с возложенной на него задачей осуществляет следующие функции:

1) создает сертификаты ключей проверки электронных подписей и выдает их заявителям, при условии установления личности заявителя либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона № 63-ФЗ;

2) осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения получателем сертификата ключа проверки электронной подписи ключом проверки электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

3) устанавливает срок действия сертификатов ключей проверки электронных подписей;

4) аннулирует выданные УЦ сертификаты ключей проверки электронных подписей;

5) выдает средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

6) ведет реестр выданных и аннулированных сертификатов ключей проверки электронных подписей (далее – реестр сертификатов), в том числе, включающий в себя информацию, содержащуюся в выданных сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей, а также об основаниях таких прекращения или аннулирования сертификатов ключей проверки электронных подписей;

7) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием сети «Интернет»;

8) создает ключи электронных подписей и ключи проверки электронных подписей по обращениям заявителей;

9) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

10) осуществляет проверку электронных подписей по обращениям участников электронного взаимодействия.

16. В целях осуществления прав и обязанностей УЦ осуществляет иную, связанную с использованием электронной подписи, деятельность.

Раздел III. ПРАВА И ОБЯЗАННОСТИ УЦ

Глава 6. ПРАВА УЦ

17. В рамках исполнения функций, предусмотренных статьями 13, 15 Федерального закона № 63-ФЗ, УЦ вправе:

1) запрашивать у заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу сертификата ключа проверки электронной подписи;

2) с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем;

3) запрашивать и получать из государственных информационных ресурсов выписку из единого государственного реестра юридических лиц в отношении заявителя – юридического лица;

4) запросить у заявителя дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными заявителем и сведениями, полученными УЦ в соответствии с частью 2.2 статьи 18 Федерального закона № 63-ФЗ;

5) не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;

6) отказать заявителю в выдаче сертификата ключа проверки электронной подписи в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона № 63-ФЗ, принимаемыми в соответствии с ним нормативными правовыми актами;

7) отказать владельцу сертификата ключа проверки электронной подписи в прекращении действия сертификата ключа проверки электронной подписи в случае, если сертификат ключа проверки электронной подписи уже аннулирован или прекратил свое действие по другим основаниям;

8) без заявления владельца сертификата ключа проверки электронной подписи прекратить действие сертификата ключа проверки электронной подписи в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата ключа проверки электронной подписи, а также невыполнения владельцем сертификата ключа проверки электронной подписи обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у УЦ достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата ключа проверки электронной подписи, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат.

18. При обработке УЦ персональных данных заявителя, установленных статьей 18 Федерального закона № 63-ФЗ, в соответствии с пунктами 2, 11 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» согласие на обработку персональных данных заявителя не требуется.

Глава 7. ОБЯЗАННОСТИ УЦ

19. УЦ обязан:

1) информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

2) обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

3) предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

4) обеспечивать конфиденциальность созданных УЦ ключей электронных подписей;

5) отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если заявителем не был подтвержден факт владения ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

6) отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;

7) вносить в создаваемые сертификаты ключей проверки электронной подписи только достоверную и актуальную информацию, подтвержденную соответствующими документами;

8) обеспечивать круглосуточную доступность реестра сертификатов в сети «Интернет», за исключением периодов планового или внепланового технического обслуживания;

9) в соответствии с частью 5 статьи 18 Федерального закона № 63-ФЗ направлять в единую систему идентификации и аутентификации (далее – ЕСИА) сведения о лице, получившем сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат), в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра) (в случае отсутствия технологической возможности (отсутствие связи при межведомственном электронном взаимодействии, проведение плановых и внеплановых работ по техническому обслуживанию, аварийные ситуации и тому подобное) сведения о лице, получившем сертификат ключа проверки электронной подписи, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате

направить в ЕСИА незамедлительно после появления технологической возможности);

10) по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в ЕСИА (в случае отсутствия технологической возможности регистрации в ЕСИА (отсутствие связи при межведомственном электронном взаимодействии, проведение плановых и внеплановых работ по техническому обслуживанию, аварийные ситуации и тому подобное) регистрация указанного в настоящем пункте лица в ЕСИА осуществляется незамедлительно после появления технологической возможности;

11) строго соблюдать срок действия ключей электронной подписи УЦ, используемых для подписания создаваемых сертификатов ключей проверки электронной подписи, распределяя сроки их действия таким образом, чтобы по окончанию таких сроков все подписанные этими ключами сертификаты ключей проверки электронной подписи прекратили свое действие.

20. Иные обязанности могут быть возложены на УЦ только путем внесения изменений в настоящий Порядок.

Раздел IV. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УЦ, В ТОМ ЧИСЛЕ ТРЕБОВАНИЯ К ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УДОСТОВЕРЯЮЩИЙ ЦЕНТР В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ

Глава 8. СОЗДАНИЕ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ДО ОБРАЩЕНИЯ В УЦ

21. Ключ электронной подписи может быть создан заявителем самостоятельно до обращения в УЦ.

22. Для создания ключа электронной подписи заявитель самостоятельно на собственном автоматизированном рабочем месте (далее – АРМ) с помощью программного средства ViPNet CSP генерирует ключевые файлы и файл запроса на создание сертификата ключа проверки электронной подписи.

После генерации ключевых файлов и файла запроса на создание сертификата ключа проверки электронной подписи заявитель копирует файл запроса на создание сертификата ключа проверки электронной подписи на ключевой носитель, после чего обращается в УЦ в целях создания сертификата ключа проверки электронной подписи.

Глава 9. ОБРАЩЕНИЕ В УЦ В ЦЕЛЯХ СОЗДАНИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ И (ИЛИ) СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

23. Заявитель подает в УЦ путем личного обращения заявление на создание сертификата ключа проверки электронной подписи по форме согласно приложению 1 к настоящему Порядку. От имени заявителя может действовать представитель.

Заявление на создание сертификата ключа проверки электронной подписи регистрируется администратором УЦ (помощником администратора) как входящий документ в Отделе в день обращения.

24. Одновременно с заявлением на создание сертификата ключа проверки электронной подписи в УЦ заявителем либо представителем заявителя представляются:

1) копия второй и третьей страниц паспорта гражданина Российской Федерации, или иного документа, удостоверяющего личность заявителя;

2) копия второй и третьей страниц паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность представителя заявителя, а также документа, удостоверяющего полномочия представителя заявителя;

3) копия акта органа, учреждения об участии заявителя в обмене электронными документами с указанием цели получения электронной подписи; в случае если заявитель является сотрудником Аппарата, представляется служебная записка в адрес начальника Отдела об участии заявителя в обмене электронными документами с указанием цели получения электронной подписи за подписью руководителя соответствующего самостоятельного структурного подразделения Аппарата;

4) согласие на обработку персональных данных заявителя (приложение 2 к настоящему Порядку);

5) копия страхового свидетельства обязательного пенсионного страхования;

6) ключевой носитель.

Указанные в настоящем пункте копии документов должны быть заверены в установленном законодательством порядке, либо должны быть представлены одновременно с предъявлением оригиналов указанных документов для их сверки и заверения администратором УЦ (помощником администратора).

25. Заявление на создание сертификата ключа проверки электронной подписи и прилагаемые документы должны соответствовать следующим требованиям:

1) документы должны быть подписаны уполномоченными лицами и (или) заверены печатями (при наличии);

2) тексты документов должны быть написаны разборчиво;

3) документы не должны иметь подчисток, приписок, зачеркнутых слов и не оговоренных в них исправлений;

4) документы не должны быть исполнены карандашом;

5) документы не должны иметь повреждений, не позволяющих однозначно истолковать их содержание;

6) копии документов должны быть качественными, не иметь нечитаемых областей.

26. В день обращения заявителя (представителя заявителя) в УЦ администратор УЦ (помощник администратора) рассматривает заявление и прилагаемые документы, а также проверяет техническую исправность ключевого носителя.

При наличии оснований, указанных в пункте 27 настоящего Порядка, заявителю (представителю заявителя) в день обращения выдается отказ в создании сертификата ключа проверки электронной подписи с указанием оснований такого отказа.

27. Основаниями отказа в создании сертификата ключа проверки электронной подписи являются:

1) заявитель не относится к категории сотрудников органов, учреждений;

2) заявление подано не по форме согласно приложению 1 к настоящему Порядку;

3) в заявлении указаны сведения, не соответствующие представленным документам;

4) представлен неполный комплект документов, указанных в пункте 24 настоящего Порядка;

5) заявление и представленные документы не соответствуют требованиям, установленным пунктом 25 настоящего Порядка;

6) несоответствие информации, содержащейся в файле запроса на создание сертификата ключа проверки электронной подписи, сведениям, указанным в заявлении на создание сертификата ключа проверки электронной подписи;

7) техническая неисправность ключевого носителя.

28. При отсутствии оснований отказа в создании сертификата ключа проверки электронной подписи в случае, если заявителем не был создан ключ электронной подписи самостоятельно до обращения в УЦ, после регистрации заявления на создание сертификата ключа проверки электронной подписи администратором УЦ (помощником администратора) осуществляется допуск заявителя к работе на АРМ УЦ для создания ключа электронной подписи.

Представитель заявителя к работе на АРМ УЦ для создания ключа электронной подписи не допускается.

29. При самостоятельном создании заявителем ключа электронной подписи с использованием АРМ УЦ используется АРМ УЦ, аттестованное на соответствие требованиям законодательства Российской Федерации по технической защите информации, размещенное в аттестованном по требованиям безопасности информации помещении, доступ в которое ограничен.

30. После допуска заявителя к работе на АРМ УЦ заявителем самостоятельно осуществляется генерация ключевых файлов и файла запроса на создание сертификата ключа проверки электронной подписи.

По просьбе заявителя администратор УЦ (помощник администратора) оказывает помощь при самостоятельном создании заявителем ключа электронной подписи с использованием АРМ УЦ, в том числе в выполнении операций на АРМ УЦ, за исключением операции ввода парольной информации.

31. При самостоятельном создании заявителем ключа электронной подписи с использованием АРМ УЦ обеспечивается соблюдение следующих требований по обеспечению безопасности информации, соответствующих

законодательству Российской Федерации по технической защите конфиденциальной информации:

1) отсутствие посторонних лиц в помещении УЦ;

2) использование средств защиты информации от неправомерных действий, в том числе средств криптографической защиты информации, имеющих действующий сертификат соответствия требованиям безопасности информации;

3) наличие действующего аттестата соответствия требованиям безопасности информации на используемое АРМ УЦ;

4) соблюдение требований организационно-распорядительной документации на используемое автоматизированное рабочее место УЦ.

32. В случаях, обусловленных технологическими особенностями используемого программного обеспечения, при создании ключей электронной подписи в составе файла ключевой криптографической информации абонентских пунктов защищенной сети допускается создание ключей электронной подписи администратором УЦ (помощником администратора) в присутствии заявителя.

33. После создания ключей электронной подписи в составе файлов ключевой криптографической информации абонентских пунктов защищенной сети администратором УЦ (помощником администратора) в присутствии заявителя файлы ключевой криптографической информации абонентских пунктов копируются на ключевой носитель, предоставленный заявителем, и удаляются с применением штатного сертифицированного средства защиты информации от несанкционированного доступа к информации с накопителя на жестком магнитном диске АРМ УЦ.

34. После генерации ключевых файлов и файла запроса на создание сертификата ключа проверки электронной подписи, указанной в пункте 30 настоящего Порядка, ключ электронной подписи, созданный самостоятельно заявителем с использованием АРМ УЦ, записывается администратором УЦ (помощником администратора) на ключевой носитель, предоставленный заявителем.

35. После создания ключа электронной подписи с использованием АРМ УЦ или в случае, если ключ электронной подписи создан заявителем самостоятельно до обращения в УЦ, администратором УЦ (помощником администратора) в течение трех рабочих дней со дня обращения заявителя (представителя заявителя) осуществляется создание сертификата ключа проверки электронной подписи путем его генерации и копирования на ключевой носитель, предоставленный заявителем (представителем заявителя).

36. После копирования сертификата ключа проверки электронной подписи на ключевой носитель, предоставленный заявителем (представителем заявителя), администратором УЦ (помощником администратора) вносится запись в журнал поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов.

37. В течение рабочего дня со дня создания сертификата ключа проверки электронной подписи администратор УЦ (помощник администратора) уведомляет об этом заявителя (представителя заявителя) по адресу

электронной почты, указанному в заявлении на создание сертификата ключа проверки электронной подписи, после чего заявитель (представитель заявителя) должен получить в УЦ сертификат ключа проверки электронной подписи.

38. Выдача ключа электронной подписи и сертификата ключа проверки электронной подписи осуществляется в УЦ при личном обращении заявителя (представителя заявителя).

По прибытии в УЦ заявитель предъявляет администратору УЦ (помощнику администратора) паспорт или иной документ, удостоверяющий личность.

В случае если получение ключа электронной подписи и сертификата ключа проверки электронной подписи осуществляется представителем заявителя, представляется паспорт или иной документ, удостоверяющий личность представителя заявителя, а также документ, удостоверяющий полномочия представителя заявителя.

39. Заявитель (представитель заявителя) расписывается в журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов за получение ключевых файлов электронной подписи, после чего администратор УЦ (помощник администратора) передает ключевой носитель заявителю (представителю заявителя).

40. Заявителю (представителю заявителя) одновременно с ключевым носителем администратор УЦ (помощник администратора) выдает правила использования средств криптографической защиты информации и электронной подписи, сущность которых сводится к определению обязанностей владельцев сертификата ключа проверки электронной подписи, в том числе по обеспечению режима конфиденциальности информации.

41. Ключевой носитель со скопированной на него информацией от УЦ выдается заявителю (представителю заявителю) лично под роспись в журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов.

42. После окончания процедуры создания сертификата ключа проверки электронной подписи администратор УЦ (помощник администратора) распечатывает сертификат ключа проверки электронной подписи на бумажном носителе в двух экземплярах. Один экземпляр выдается заявителю (представителю заявителя), второй экземпляр с подписью заявителя (представителя заявителя) об ознакомлении с содержанием сертификата ключа проверки электронной подписи остается в УЦ.

Глава 10. ОСУЩЕСТВЛЕНИЕ ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УЦ

43. Плановая смена ключей электронной подписи УЦ осуществляется в связи с истечением срока действия ключей электронной подписи УЦ.

44. Срок действия ключей электронной подписи УЦ составляет 5 лет.

45. Плановая смена ключей электронной подписи УЦ осуществляется администратором УЦ (помощником администратора) в соответствии технической документацией на применяемое программное обеспечение УЦ.

46. Информирование владельцев сертификатов ключей проверки электронной подписи об осуществлении плановой смены ключей электронной подписи УЦ осуществляется путем размещения соответствующего информационного сообщения и нового сертификата ключа проверки электронной подписи УЦ в сети «Интернет» по адресу: http://inform.irkobl.ru.

47. Доверенным способом получения нового сертификата ключа проверки электронной подписи УЦ является скачивание файла нового сертификата ключа проверки электронной подписи в сети «Интернет» по адресу: http://inform.irkobl.ru.

Глава 11. СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УЦ ПРИ ИХ КОМПРОМЕТАЦИИ

48. Внеплановая смена ключей электронной подписи УЦ осуществляется в случае:

1) компрометации ключа электронной подписи УЦ;

2) угрозы компрометации ключа электронной подписи УЦ.

49. Внеплановая смена ключей электронной подписи УЦ осуществляется администратором УЦ (помощником администратора) в соответствии технической документацией на применяемое программное обеспечение УЦ.

50. Внеплановая смена ключей электронной подписи УЦ осуществляется администратором УЦ (помощником администратора) в течение 1 рабочего дня после выявления компрометации ключа электронной подписи УЦ или угрозы компрометации ключа электронной подписи УЦ.

51. Одновременно со сменой ключей электронной подписи УЦ прекращается действие всех сертификатов ключей проверки электронной подписи, подписанных этим ключом электронной подписи, с занесением сведений об этих сертификатах ключей проверки электронной подписи в реестр сертификатов.

52. Информирование владельцев сертификатов ключей проверки электронной подписи об осуществлении внеплановой смены ключей электронной подписи УЦ осуществляется путем размещения соответствующего информационного сообщения и нового сертификата ключа проверки электронной подписи УЦ в сети «Интернет» по адресу: http://inform.irkobl.ru.

53. В случае осуществления внеплановой смены ключей электронной подписи УЦ, УЦ безвозмездно создает сертификаты ключей проверки электронной подписи для всех владельцев сертификатов ключей проверки электронной подписи, чьи сертификаты ключей проверки электронной подписи прекращают действие в связи с внеплановой сменой.

Глава 12. СМЕНА КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ПО ЗАЯВЛЕНИЮ ВЛАДЕЛЬЦА СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

54. Администратор УЦ (помощник администратора) осуществляет смену ключа электронной подписи владельца сертификата ключа проверки электронной подписи и создание нового сертификата ключа проверки электронной подписи в соответствии с главами 8, 9 настоящего Порядка на основании заявления на создание сертификата ключа проверки электронной подписи (приложение 1 к настоящему Порядку) без представления документов, указанных в пункте 24 настоящего Порядка.

55. При смене ключа электронной подписи владельца сертификата ключа проверки электронной подписи заявление на создание сертификата ключа проверки электронной подписи может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата ключа проверки электронной подписи и направлено по адресу электронной почты, указанному в подпункте 5 пункта 9 настоящего Порядка либо предоставляется на ключевом носителе.

56. Если смена ключа электронной подписи владельца сертификата ключа проверки электронной подписи связана с его компрометацией или угрозой компрометации и из заявления точно следует, ключ какого владельца сертификата ключа проверки электронной подписи подлежит смене, то смена осуществляется и в том случае, если заявление подано с нарушением отдельных требований к заявлению.

57. Процедура выдачи сертификата ключа проверки электронной подписи и (при необходимости) ключа электронной подписи владельцу сертификата ключа проверки электронной подписи, в том числе в электронной форме, осуществляется в соответствии с главами 8, 9 настоящего Порядка с соблюдением положений статьи 18 Федерального закона № 63-ФЗ.

Глава 13. ПОДТВЕРЖДЕНИЕ ДЕЙСТВИТЕЛЬНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ, ИСПОЛЬЗОВАННОЙ ДЛЯ ПОДПИСАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

58. Заявление на подтверждение действительности электронной подписи, использованной для подписания электронных документов (далее – заявление на подтверждение действительности электронной подписи), по форме согласно приложению 3 к настоящему Порядку, оформленное на бумажном носителе, подается заявителем в УЦ путем личного обращения либо посредством почтового направления по адресу, указанному в пункте 9 настоящего Порядка.

59. Заявление на подтверждение действительности электронной подписи регистрируется администратором УЦ (помощником администратора) в день поступления как входящий документ в Отделе.

60. Заявление на подтверждение действительности электронной подписи на бумажном носителе должно соответствовать требованиям, указанным в пункте 25 настоящего Порядка.

61. К заявлению на подтверждение действительности электронной подписи заявитель прилагает ключевой носитель, содержащий электронный документ, электронную подпись в котором необходимо проверить на предмет действительности.

62. В день подачи заявления на подтверждение действительности электронной подписи администратор УЦ (помощник администратора) осуществляет рассмотрение указанного заявления и проводит проверку технической исправности ключевого носителя.

63. В случае если заявление на подтверждение действительности электронной подписи не соответствует требованиям пункта 25 настоящего Порядка, либо выявлена неисправность ключевого носителя администратор УЦ (помощник администратора) не позднее трех рабочих дней со дня регистрации указанного заявления в УЦ возвращается заявителю ключевой носитель вместе с заявлением на подтверждение действительности электронной подписи по адресу, указанному в заявлении на подтверждение действительности электронной подписи.

64. Срок подтверждения действительности электронной подписи в электронном документе не может превышать трех рабочих дней со дня регистрации заявления на подтверждение действительности электронной подписи в Отделе.

65. В случае принятия положительного решения по результатам рассмотрения заявления на подтверждение действительности электронной подписи и проверки ключевого носителя администратор УЦ (помощник администратора) в срок до трех рабочих дней со дня регистрации в УЦ заявления на подтверждение действительности электронной подписи осуществляет процедуру проверки действительности всех сертификатов ключей проверки электронных подписей, включенных в цепочку проверки для сертификата ключа проверки электронной подписи, указанного в заявлении на подтверждение действительности электронной подписи, до сертификата аккредитованного УЦ, выданного ему головным УЦ.

66. Подтверждение действительности электронной подписи осуществляется на безвозмездной основе.

67. По результатам проверки, указанной в пункте 65 настоящего Порядка, заявителю выдается заключение о действительности либо недействительности электронной подписи, использованной для подписания электронного документа, представленного заявителем на ключевом носителе.

Глава 14. ПРОЦЕДУРЫ, ОСУЩЕСТВЛЯЕМЫЕ ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ И АННУЛИРОВАНИИ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

68. Сертификат ключа проверки электронной подписи прекращает свое действие:

1) по истечении срока его действия;

2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью;

3) в случае прекращения деятельности УЦ без передачи его функций другим лицам;

4) в иных случаях, установленных в настоящем Порядке в соответствии с законодательством Российской Федерации в области электронной подписи.

69. Сертификат ключа проверки электронной подписи признается аннулированным, в случае если:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате ключа проверки электронной подписи;

2) установлено, что содержащийся в сертификате ключа проверки электронной подписи ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

3) вступило в силу решение суда, которым установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

70. Владелец сертификата ключа проверки электронной подписи (далее – владелец сертификата) подает в УЦ заявление о прекращении действия сертификата ключа проверки электронной подписи по форме согласно приложению 4 к настоящему Порядку. От имени владельца сертификата может действовать представитель, действующий на основании закона или доверенности.

71. Заявление о прекращении действия сертификата ключа проверки электронной подписи может быть оформлено как на бумажном носителе, так и в форме электронного документа.

72. Заявление о прекращении действия сертификата ключа проверки электронной подписи, оформленное на бумажном носителе, подается владельцем сертификата (его представителем) в УЦ путем личного обращения либо посредством почтового направления по адресу, указанному в пункте 9 настоящего Порядка.

Заявление о прекращении действия сертификата ключа проверки электронной подписи в форме электронного документа направляется по адресу электронной почты, указанному в подпункте 5 пункта 9 настоящего Порядка, либо предоставляется на ключевом носителе.

73. Заявление о прекращении действия сертификата ключа проверки электронной подписи регистрируется администратором УЦ (помощником администратора) как входящий документ в Отделе в день обращения.

74. Заявление о прекращении действия сертификата ключа проверки электронной подписи, оформленное на бумажном носителе, должно соответствовать требованиям, указанным в пункте 25 настоящего Порядка.

75. Заявление о прекращении действия сертификата ключа проверки электронной подписи, направленное в форме электронного документа, должно соответствовать следующим требованиям:

1) заявление о прекращении действия сертификата ключа проверки электронной подписи должно быть оформлено в текстовом редакторе Word с использованием шрифта Times New Roman размером № 14 на белом фоне и направлено в формате RTF;

2) о прекращении действия сертификата ключа проверки электронной подписи должно не иметь нечитаемых областей;

3) файлы и информация, содержащаяся в них, должны быть доступными для работы, не должны быть защищены от копирования и печати, не должны содержать интерактивные и мультимедийные элементы, внедренные сценарии на языке JavaScript или любых других языках программирования;

4) размер одного файла, содержащего электронную копию документа, не должен превышать 30 Мб.

76. В случае если заявление о прекращении действия сертификата ключа проверки электронной подписи не соответствует требованиям пунктов 74-75 настоящего Порядка владельцу сертификата (его представителю) не позднее трех рабочих дней со дня регистрации в УЦ указанного заявления по адресу, указанному в заявлении о прекращении действия сертификата ключа проверки электронной подписи, направляется уведомление об отказе в прекращении действия сертификата ключа проверки электронной подписи.

77. При подаче заявления о прекращении действия сертификата ключа проверки электронной подписи, требуется согласование указанного заявления с руководителем органа (учреждения), сотрудник которого намерен прекратить действие сертификата ключа проверки электронной подписи.

В случае если заявитель является сотрудником Аппарата, представляется служебная записка в адрес начальника Отдела о прекращении действия сертификата ключа проверки электронной подписи за подписью руководителя соответствующего самостоятельного структурного подразделения Аппарата;

78. При личном обращении владельца сертификата в УЦ администратор УЦ (помощник администратора) устанавливает личность владельца сертификата по паспорту или иному документу, удостоверяющему личность владельца сертификата.

79. При обращении в УЦ представителя владельца сертификата, его личность устанавливается по паспорту или иному документу, удостоверяющему личность, а также документу, удостоверяющему полномочия представителя владельца сертификата. В качестве документа, удостоверяющего полномочия на осуществление действий от имени владельца сертификата, может быть представлена оформленная в соответствии с законодательством Российской Федерации доверенность.

80. В случае принятия положительного решения по результатам рассмотрения заявления о прекращении действия сертификата ключа проверки электронной подписи администратор УЦ (помощник администратора) в течение трех рабочих дней со дня регистрации в УЦ заявления о прекращении

действия сертификата ключа проверки электронной подписи аннулирует сертификат ключа проверки электронной подписи при помощи специализированных программных средств и уведомляет об этом владельца аннулированного сертификата ключа проверки электронной подписи по адресу, указанному в заявлении о прекращении действия сертификата ключа проверки электронной подписи.

81. После проведения процедуры аннулирования сертификата ключа проверки электронной подписи администратор УЦ (помощник администратора) вносит информацию об аннулированном сертификате ключа проверки электронной подписи в файл реестра сертификатов, подписывает файл реестра сертификатов усиленной квалифицированной электронной подписью и публикует файл реестра сертификатов в сети «Интернет» по адресу: http://inform.irkobl.ru.

82. Срок внесения информации о прекращении действия или аннулировании сертификата ключа проверки электронной подписи в реестр сертификатов не может превышать 12 часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона № 63-ФЗ, или в течение 12 часов с момента, когда администратору УЦ (помощнику администратора) стало известно или должно было стать известно о наступлении таких обстоятельств.

Глава 15. ВЕДЕНИЕ РЕЕСТРА СЕРТИФИКАТОВ

83. Реестр сертификатов ведется в текстовом редакторе Microsoft Excel с использованием шрифта Times New Roman.

84. Реестр сертификатов размещается в сети «Интернет» по адресу: http://inform.irkobl.ru.

85. Резервная копия реестра сертификатов хранится на АРМ администратора УЦ.

86. Информация о прекращении действия или аннулировании сертификата ключа проверки электронной подписи в реестр сертификатов вносится администратором УЦ (помощником администратора) незамедлительно после проведения соответствующих операций в УЦ.

87. В случае отсутствия технологической возможности внесения информации (отсутствие связи, аварийная ситуация и так далее) информация о прекращении действия или аннулировании сертификата ключа проверки электронной подписи в реестр сертификатов вносится администратором УЦ (помощником администратора) незамедлительно после появления такой возможности.

Глава 16. ПЛАНОВОЕ И ВНЕПЛАНОВОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ РЕЕСТРА СЕРТИФИКАТОВ

88. Плановое техническое обслуживание реестра сертификатов проводится при проведении планового технического обслуживания в сети «Интернет» по адресу: http://inform.irkobl.ru.

89. Максимальный срок планового обслуживания реестра сертификатов составляет один рабочий день.

90. Внеплановое техническое обслуживание реестра сертификатов осуществляется при возникновении нештатных ситуаций.

91. Максимальный срок внепланового технического обслуживания реестра сертификатов составляет один рабочий день.

92. Уведомление о проведении технического обслуживания реестра сертификатов осуществляется посредством размещения соответствующего информационного сообщения в сети «Интернет» по адресу: http://inform.irkobl.ru.

Раздел V. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УЦ

Глава 17. ИНФОРМИРОВАНИЕ ЗАЯВИТЕЛЕЙ ОБ УСЛОВИЯХ И О ПОРЯДКЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И СРЕДСТВ ЭЛЕКТРОННОЙ ПОДПИСИ, О РИСКАХ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПОДПИСЕЙ, И О МЕРАХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И ИХ ПРОВЕРКИ

93. В момент получения заявителем электронной подписи администратор УЦ (помощник администратора) информирует заявителя в письменной форме об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, путем выдачи соответствующей памятки под роспись.

94. Памятка об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки также размещается в сети «Интернет» по адресу: http://inform.irkobl.ru.

Глава 18. ОБЕСПЕЧЕНИЕ АКТУАЛЬНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В РЕЕСТРЕ СЕРТИФИКАТОВ, И ЕЕ ЗАЩИТЫ ОТ НЕПРАВОМЕРНОГО ДОСТУПА, УНИЧТОЖЕНИЯ, МОДИФИКАЦИИ, БЛОКИРОВАНИЯ, ИНЫХ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ

95. Администратор УЦ (помощник администратора) обеспечивает актуальность информации, содержащейся в реестре сертификатов, путем ежедневной сверки в рабочие дни в 16:00 часов со сведениями, имеющимися в базе данных программного обеспечения УЦ.

96. УЦ обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий путем проведения полного комплекса организационно-технических мероприятий по защите информации

от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в отношении официального портала Иркутской области (в сети «Интернет» по адресу: http://inform.irkobl.ru) и на АРМ администратора УЦ и помощника администратора в соответствии с руководящими документами Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Глава 19. ОБЕСПЕЧЕНИЕ КРУГЛОСУТОЧНОЙ ДОСТУПНОСТИ РЕЕСТРА СЕРТИФИКАТОВ В СЕТИ «ИНТЕРНЕТ», ЗА ИСКЛЮЧЕНИЕМ ПЕРИОДОВ ПЛАНОВОГО ИЛИ ВНЕПЛАНОВОГО ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ РЕЕСТРА СЕРТИФИКАТОВ

97. УЦ обеспечивает круглосуточную доступность реестра сертификатов в сети «Интернет» по адресу: http://inform.irkobl.ru, за исключением периодов планового или внепланового технического обслуживания в соответствии с главой 16 настоящего Порядка.

98. Круглосуточная доступность сайта http://inform.irkobl.ru обеспечивается областным государственным автономным учреждением «Информационно-технический центр Иркутской области».

Глава 20. ПОРЯДОК ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ СОЗДАННЫХ УЦ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

99. Конфиденциальность созданных УЦ ключей электронных подписей достигается следующими мероприятиями:

1) исключением нахождения посторонних лиц в помещении УЦ в момент формирования ключа электронной подписи;

2) незамедлительным гарантированным удалением администратором УЦ (помощником администратора) ключей электронной подписи с накопителя на жестком магнитном диске АРМ УЦ с использованием сертифицированного средства защиты информации от несанкционированного доступа;

3) использованием сертифицированных по требованиям безопасности информации средств защиты информации на АРМ УЦ, аттестованного по требованиям безопасности информации;

4) безусловным выполнением требований организационно-распорядительных документов на АРМ УЦ;

5) инструктированием пользователя о правилах защиты информации при обращении с ключевыми носителями информации, содержащими ключ электронной подписи.

100. После получения в установленном порядке ключей электронной подписи, созданных в УЦ, обеспечение их конфиденциальности осуществляется заявителем.

Глава 21. ОСУЩЕСТВЛЕНИЕ РЕГИСТРАЦИИ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ В ЕСИА

101. Администратор УЦ (помощник администратора) направляет в ЕСИА сведения о лице, получившем сертификат ключа проверки электронной подписи, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате ключа проверки электронной подписи, содержащем уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра.

102. В случае отсутствия технологической возможности (проведение плановых и внеплановых работ по техническому обслуживанию, аварийные ситуации и другое) сведения о лице, получившем сертификат ключа проверки электронной подписи, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате ключа проверки электронной подписи администратор УЦ (помощник администратора) направляет в ЕСИА незамедлительно после появления технологической возможности.

Глава 22. ОСУЩЕСТВЛЕНИЕ ПО ЖЕЛАНИЮ ЛИЦА, КОТОРОМУ ВЫДАН КВАЛИФИЦИРОВАННЫЙ СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ, БЕЗВОЗМЕЗДНОЙ РЕГИСТРАЦИИ УКАЗАННОГО ЛИЦА В ЕСИА

103. По желанию лица, которому выдан квалифицированный сертификат ключа проверки электронной подписи, администратор УЦ (помощник администратора) безвозмездно осуществляет регистрацию указанного лица в ЕСИА.

104. В случае отсутствия технологической возможности регистрации в ЕСИА (проведение плановых и внеплановых работ по техническому обслуживанию, аварийные ситуации и другое) лица, указанного в пункте 103 настоящего Порядка, администратор УЦ (помощник администратора) незамедлительно осуществляет регистрацию после появления технологической возможности.

Глава 23. ПРЕДОСТАВЛЕНИЕ БЕЗВОЗМЕЗДНО ЛЮБОМУ ЛИЦУ ПО ЕГО ОБРАЩЕНИЮ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В РЕЕСТРЕ СЕРТИФИКАТОВ, В ТОМ ЧИСЛЕ ИНФОРМАЦИИ ОБ АНУЛЛИРОВАНИИ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

105. Реестр сертификатов размещается в сети «Интернет» по адресу: http://inform.irkobl.ru, тем самым обеспечивается доступ к нему неограниченного круга лиц.

106. В случае поступления в адрес УЦ обращения о предоставлении информации из реестра сертификатов, УЦ обязан направить запрашиваемую информацию в срок, не превышающий семи рабочих дней с момента поступления обращения в УЦ, по адресу, указанному в обращении.

Обращение о предоставлении информации из реестра сертификатов регистрируется администратором УЦ (помощником администратора) как входящий документ в Отделе в день обращения.

107. В случае если в обращении о предоставлении информации из реестра квалифицированных сертификатов ключей проверки электронных подписей содержится информация о направлении ответа посредством информационно-телекоммуникационных сетей, администратор УЦ (помощник администратора) направляет ответ, подписанный усиленной квалифицированной электронной подписью в адрес заявителя посредством информационно-телекоммуникационных сетей в срок, не превышающий 24 часов с момента поступления указанного обращения в УЦ.

Первый заместитель руководителя аппарата Губернатора Иркутской области и Правительства Иркутской области А.В. Южаков