Приложение № 5

к Порядку реализации АО «Торговый дом «ПЕРЕКРЕСТОК» функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утверждённому приказом от 16.04.2024 № 3-1-100/002425-24

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1 Общие положения

1.1. Настоящее руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее – руководство) подготовлено в соответствии с частью 4 статьи 18 ФЗ «Об электронной подписи».

1.2. Руководство предназначено для официального информирования владельца квалифицированного сертификата ключа проверки электронной подписи, выдаваемого УЦ, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

2. Риски, связанных с использованием электронных подписей

2.1. Основными рисками, связанными с использованием электронной подписи, являются:

2.1.1. риски, связанные с нарушением целостности электронного документа и возможностью отказа от него.

Данные риски могут быть связаны с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, подписавшее электронный документ квалифицированной электронной подписью, или лицо, осуществляющее проверку такой электронной подписи, может заявить о том, что содержание электронного документа было изменено после его подписания и электронный документ не соответствует тому документу, который был подписан квалифицированной электронной подписью;

2.1.2. риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу квалифицированного сертификата ключа проверки электронной подписи (далее – владелец квалифицированного сертификата).

Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что квалифицированная электронная подпись, содержащаяся в электронном документе, не принадлежит данному владельцу квалифицированного сертификата;

2.1.3. риски, связанные с признанием юридической силы электронного документа, подписанного квалифицированной электронной подписью.

Одна из сторон может заявить о том, что подписанный квалифицированной электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

2.1.4. риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца).

В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, участником электронного взаимодействия может быть принят в исполнение подписаны квалифицированной электронной подписью документ, порождающий юридически значимые последствия.

Нарушение конфиденциальности ключа электронной подписи (в том числе нарушение правил хранения ключа электронной подписи, несоблюдение требований Порядка УЦ в случаях прекращения либо аннулирования действия сертификата ключа подписи) или нарушение правил эксплуатации средств квалифицированной электронной подписи может привести к нарушению прав и законных интересов владельца квалифицированного сертификата и/или третьих лиц.

2.1.5. риски, связанные с использованием несертифицированных средств, предназначенных для защиты информации.

Использование для создания и проверки квалифицированных электронных подписей, создания ключа электронной подписи и ключа проверки электронной подписи несертифицированных в соответствии с правилами сертификации Российской Федерации средств электронной подписи, и применение этих средств в нарушение правил, установленных нормативными правовыми актами Российской Федерации, а также эксплуатационной документации к средствам электронной подписи, может повлечь административную ответственность.

2.1.6. риски, связанные с определением полномочий лица, подписавшего электронной подписью документ.

В случае, если участниками электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит квалифицированную электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение.

2.1.7. риски, связанные с использованием сертификатов ключей проверки электронной подписи и ключей электронной подписи, прекративших своё действие.

В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, а также в случае использования сертификата ключа проверки электронной подписи, который стал недействующим на день проверки электронной подписи, сторона, получившая подписанный квалифицированной электронной подписью документ, может заявить о непризнании такого электронного документа.

2.1.8. риски, связанные с неактуальностью данных в сертификате.

В случае, если в период действия сертификата персональных данных владельца произошли изменения, необходимо обратиться в УЦ для получения нового сертификата. В противном случае, любой электронный документ, подписанный данным сертификатом, может быть признан недействительным.

3. Меры, необходимые для обеспечения безопасности электронных подписей и их проверки.

3.1. Правовые и организационно-технические мероприятия для при осуществлении электронного взаимодействия с использованием электронной подписи.

3.1.1. В целях снижения вероятности возникновения и реализации указанных рисков владельцу квалифицированного сертификата необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием электронной подписи.

3.1.2. Электронное взаимодействие с использованием электронной подписи и сертифицированных средств электронной подписи, осуществляется с учетом требований ФЗ

«Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, в том числе:

- Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 N 152;

- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66, в части эксплуатации средств криптографической защиты информации.

3.1.3. Средства усиленной квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство усиленной квалифицированной электронной подписи.

3.1.4. На компьютерах с установленными средствами усиленной квалифицированной электронной подписи должно использоваться только лицензионное программное обеспечение. Для предотвращения заражения компьютера с установленными средствами усиленной квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

Владелец квалифицированного сертификата несет ответственность за то, чтобы на компьютере, на котором установлены средства криптографической защиты информации, не было установлено и не эксплуатировалось программное обеспечение (в том числе, - вирусы), которые могут нарушить функционирование программных средств криптографической защиты информации. При обнаружении на рабочем месте, оборудованном средствами криптографической защиты информации, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

3.1.5. Помещения, в которых установлены средства усиленной квалифицированной электронной подписи или хранятся носители ключей электронной подписи, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

В помещениях, где установлены и применяются средства усиленной квалифицированной электронной подписи для хранения носителей ключей электронной подписи, эксплуатационной и технической документации, дистрибутивов программного обеспечения средств усиленной квалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, в целях предотвращения несанкционированного доступа к средствам усиленной квалифицированной электронной подписи.

Используемые или хранимые средства усиленной квалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители Ключей электронной подписи подлежат поэкземплярному учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

3.2. Владелец квалифицированного сертификата обязан соблюдать определенные меры для обеспечения безопасности своих действий:

3.2.1. не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

3.2.2. для хранения ключа электронной подписи применять защищенный носитель информации, совместимый одновременно со средством электронной подписи, применяемым владельцем квалифицированного сертификата, и средствами УЦ;

3.2.3. применять для создания электронной подписи только действующий ключ электронной подписи;

3.2.4. прекратить использование ключа электронной подписи и немедленно обратиться в УЦ с заявлением о прекращении действия квалифицированного сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи;

3.2.5. не использовать сертификат ключа проверки электронной подписи, заявление на прекращение действия, которого подано в УЦ, в течение времени, исчисляемого с момента подачи заявления на прекращение действия сертификата в УЦ по момент официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;

3.2.6. не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован;

3.2.7. использовать для создания и проверки квалифицированных электронных подписей, создания ключа электронной подписи и ключа проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи, и применять эти средства в соответствии с правилами, установленными нормативными правовыми актами Российской Федерации;

3.2.8. использовать при проверке электронной подписи в электронных документах актуальную информацию о сертификатах ключей проверки электронных подписей, которые на данный момент времени аннулированы, действие которых прекращено, содержащуюся в списке отозванных сертификатов, размещенном в сети Интернет на сайте УЦ;

3.2.9. в случае изменения персональных данных, включенных в сертификат ключа проверки электронной подписи, необходимо обратиться в УЦ с целью замены данного сертификата.

3.3. С учетом указанных правовых и организационно-технических мероприятий, обязанностей, владельцу квалифицированного сертификата запрещается:

3.3.1. осуществлять несанкционированное копирование ключевых носителей;

3.3.2. оставлять без контроля вычислительные средства, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

3.3.3. вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;

3.3.4. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

3.3.5. записывать на ключевые носители постороннюю информацию;

3.3.6. подключать к компьютеру с установленным средством квалифицированной электронной подписи дополнительные устройства и соединители;

3.4. Меры по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи.

3.4.1. Владелец квалифицированного сертификата обеспечивает безопасность ключей квалифицированной электронной подписи с помощью следующих методов:

3.4.1.1. ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним;

3.4.1.2. ключевые носители должны иметь маркировку с учетным номером.

3.4.2. Владелец квалифицированного сертификата обеспечивает безопасное и надежное хранение и обращение с ключевой информацией и ключевыми носителями. Это достигается за счет соблюдения следующих способов и мер безопасности, которые гарантируют сохранность и конфиденциальность данных:

3.4.2.1. недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей);

3.4.2.2. размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками;

3.4.2.3. носители ключевой информации должны использоваться только владельцем квалифицированного сертификата и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.);

3.4.2.4. носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

3.4.2.5. на носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

3.4.3. Владелец квалифицированного сертификата обеспечивает безопасность автоматизированного рабочего места с установленными средствами квалифицированной электронной подписи.

3.4.3.1. С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям информационной безопасности;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

- должна быть активирована регистрация событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода владельца квалифицированного сертификата с автоматизированного рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред владельцу квалифицированного сертификата и УЦ, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.

3.4.4. В случае нарушения конфиденциальности ключей электронной подписи владелец квалифицированного сертификата, с учетом условий Порядка УЦ:

- незамедлительно обращается в УЦ;

- прекращение действия квалифицированного сертификата осуществляется по заявлению, которое оформляется в соответствии с Приложением № 3 к Порядку УЦ. Заявление о прекращении действия квалифицированного сертификата может подаваться в УЦ как на бумажном носителе, так и направляется в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.