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

1. Общие положения

1.1. Настоящее руководство разработано в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» и предназначено для лиц, заинтересованных в получении или владеющих квалифицированным сертификатом ключа проверки электронной подписи, создаваемым Государственным бюджетным учреждением «Центр информационных технологий Волгоградской области» (далее – Удостоверяющий центр),

1.2. Руководство является средством официального информирования об условиях, рисках и порядке использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее – средства ЭП), а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

1.3. Применение квалифицированной электронной подписи в государственных и иных информационных системах, а также в системах юридически значимого электронного документооборота, сопровождаются в том числе следующими рисками:

1) финансовые убытки (в том числе штрафы и т.п.);
2) репутационные риски;
3) нарушение сроков оказания государственных и муниципальных услуг;
4) нарушение правильного функционирования информационных систем.

1.4. Риски, связанные с применение квалифицированной электронной подписи, возникают вследствие возможности признания недействительности сделок, совершенных с использованием квалифицированной электронной подписи, недействительности документов, подписанных квалифицированной электронной подписью при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка квалифицированной электронной подписи.

1.5. В целях снижения рисков необходимо выполнение приведенных в настоящем руководстве организационно-технических и административных мер по обеспечению безопасного функционирования средств обработки и передачи информации.

1.6. В соответствии с правилами функционирования информационных системах и систем обмена электронными документами, а также требованиями по эксплуатации средств ЭП могут быть установлены дополнительные требования по обеспечению их безопасной эксплуатации.

2. Требования к организация режима обеспечения безопасности помещений, в которых эксплуатируются средства квалифицированной электронной подписи

2.1. При эксплуатации средств ЭП должны быть реализованы меры, препятствующие возможности неконтролируемого проникновения или пребывания в помещениях, где размещены (или хранятся) используемые средства ЭП и (или) носители ключевой, аутентифицирующей и парольной информации средств ЭП (далее - Помещения), лиц, не имеющих права доступа в Помещения. Указанные меры могут быть реализованы, в том числе, путем:

а) оснащения Помещений входными дверьми с замками, обеспечения закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в Помещения.

2.2. В случае необходимости присутствия посторонних лиц в Помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной

подписи, средства обработки информации и передаваемую информацию.

2.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им документов и сведений, включая ключи электронной подписи.

3. Требования по защите информации от несанкционированного доступа средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств ЭП должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на средствах вычислительной техники с установленными средствами ЭП должна быть установлена только одна операционная система;
- все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
    - системному реестру;
    - файлам и каталогам;
    - временным файлам;
    - журналам системы;
    - файлам подкачки;
    - кэшируемой информации (пароли и т.п.);
    - отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

- организовать стирание (по окончании сеанса работы средств электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

3.1.4. В случае подключения технических средств с установленными средствами ЭП к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в т.ч. Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства ЭП и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

3.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита.
- комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств ЭП;
- работать со средствами электронной подписи при включенных в техническое средство штатных средствах выхода в радиоканал;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами ЭП без контроля после ввода ключевой информации;
- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

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

4.1. Меры защиты ключей квалифицированной электронной подписи

Ключи квалифицированной электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством ЭП согласно технической и эксплуатационной документации к ним.

Ключи квалифицированной электронной подписи на ключевом носителе должны быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство ЭП.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами, по электронной почте сети Интернет или по внутренней электронной почте (кроме файлов квалифицированных сертификатов ключей проверки электронной подписи).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token, Рутокен, ESMART Token и др.). Размещение ключевой информации в реестре Windows, на локальном или сетевом диске, а также во встроенной памяти технического средства с

установленными средствами ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен подключаться в считывающее устройство только на время выполнения средствами 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.

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

4.3. Обеспечение безопасности средств вычислительной техники с установленными средствами ЭП

С целью контроля исходящего и входящего подозрительного трафика, средства вычислительной техники с установленными средствами ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку во внешние сети информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами ЭП третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;
- должна быть активирована подсистема регистрации событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук, планшет). Если выбран переносной компьютер, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства ЭП, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства ЭП, журналы работы систем обмена электронными документами и т.д.).

5. Действия при компрометации ключей квалифицированной электронной подписи

5.1. К событиям, относящимся к компрометации ключей квалифицированной электронной подписи, относятся следующие ситуации:

1) ознакомление неуполномоченного лица (лиц) с ключами квалифицированной электронной подписи;

2) утрата ключевого носителя с ключами квалифицированной электронной подписи;

3) увольнение пользователя ключа квалифицированной электронной подписи;

4) нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для хранения ключевых носителей;

5) утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей;

6) случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника, утрата ключевого носителя с последующим обнаружением).

5.2. В случае компрометации ключей квалифицированной электронной подписи владелец квалифицированного сертификата ключа проверки электронной подписи должен:

1) прекратить использование ключа квалифицированной электронной подписи и соответствующего квалифицированного сертификата ключа проверки электронной подписи;

2) незамедлительно обратиться в Удостоверяющий центр для аннулирования (прекращения действия) соответствующего квалифицированного сертификата ключа проверки электронной подписи и получения (при необходимости) нового квалифицированного сертификата ключа проверки электронной подписи в соответствии с Регламентом оказания услуг Удостоверяющего центра (http://ca.citvo.ru/Portals/2/Files/regdocs/RegCA.pdf).