**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**
**(БАНК РОССИИ)**

УТВЕРЖДАЮ
Заместитель Председателя
Банка России

_____ Г.А. Зубарев
«____» _____2021 г.

# Автоматизированная система аккредитованного удостоверяющего центра Центрального банка Российской Федерации

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

на 9 листах

Москва, 2021 г.

## 1 Общие положения

Настоящее руководство подготовлено в соответствии с частью 4 статьи 18 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон) и предназначено для официального информирования владельцев квалифицированных сертификатов ключей проверки электронной подписи (далее – квалифицированный сертификат), выдаваемых аккредитованным удостоверяющий центром Банка России, о рисках, условиях и правилах применения электронной подписи (далее – ЭП) и средств квалифицированной ЭП, а также о мерах, необходимых для обеспечения безопасности использования квалифицированной ЭП и средств квалифицированной ЭП.

Определение понятий «квалифицированная электронная подпись», «средство электронной подписи» содержится в статье 2 Федерального закона.

При использовании в правоотношениях квалифицированной ЭП, использовании и эксплуатации средств квалифицированной ЭП владельцы квалифицированных сертификатов и средств квалифицированной ЭП должны соблюдать требования:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»
- 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 № 152;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66;
- эксплуатационной документации на средства ЭП;
- настоящего руководства.

## 2 Требования к помещениям и размещению средств ЭП

При размещении в помещении средств вычислительной техники (далее – СВТ) с установленными на них средствами квалифицированной ЭП:

- должны быть предусмотрены меры, исключающие возможность несанкционированного доступа и пребывания в помещении лиц, не имеющих допуск к работе в этом помещении. При необходимости пребывания указанных лиц в помещении должен быть обеспечен контроль их действий в целях недопущения с их стороны несанкционированных воздействий на средства ЭП, иные средства криптографической защиты информации (далее – СКЗИ), ключевую информацию;
- входные двери помещений должны быть оснащены устройствами, обеспечивающими контроль доступа в нерабочее время.

## 3 Требования по установке и эксплуатации средств квалифицированной ЭП, общесистемного и специального программного обеспечения

3.1 При установке и использовании на СВТ средств квалифицированной ЭП должны выполняться следующие меры по защите информации:

1) в отношении СВТ должны соблюдаться правила:
   - не допускается установка операционных систем (далее – ОС), не предусмотренных документацией на средства ЭП, либо измененных или отладочных версий ОС, указанных в документации;
   - не допускается установка программных средств, реализующих функции удаленного управления, администрирование, модификацию ОС и её настроек, а также среды разработки;
   - не допускается установка нескольких ОС;
   - неиспользуемые ресурсы СВТ должны быть отключены (протоколы, сервисы и т.п.);

- реализованные на СВТ режимы безопасности должны быть настроены на максимальный уровень;
- зарегистрированным пользователям СВТ назначаются минимально возможные для нормальной работы права;
- предоставление минимальных прав доступа к ресурсам СВТ, включая доступ к системному реестру, файлам и каталогам, временным файлам, файлам подкачки и т.п.

2) на СВТ необходимо:
   - по окончании сеанса работы с использованием средств квалифицированной ЭП удалить временные файлы и файлы подкачки. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
   - исключить установку и выполнение на СВТ программ, позволяющих повысить привилегии пользователям СВТ;
   - регулярно устанавливать обновления ОС, прикладных систем, антивирусные базы.
3) на СВТ следует использовать парольную защиту (для входа в ОС, BIOS, при шифровании на пароле и т.д.), обеспечивающую возможность реализации следующей политики:
   - длина пароля должна быть не менее 8 символов;
   - в последовательности символов пароля 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 распространенные сокращения (USER, ADMIN, root, и т.д.);

- осуществлять периодическую смену пароля в соответствии с регламентом, установленным в технической документации организации (рекомендуется не реже 1 раза в год);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

3.2 При необходимости подключения СВТ с установленными на них средствами квалифицированной ЭП к общедоступным сетям передачи данных (в том числе сети Интернет) такое подключение необходимо осуществлять при использовании средств защиты от сетевых атак. При работе на указанных СВТ необходимо исключить возможность открытия и исполнения файлов и иных получаемых по сети объектов без предварительной их проверки сертифицированными средствами антивирусной защиты.

3.3 Необходимо организовать сбор событий (лог-файлы) в отношении СВТ, на которых установлены средства ЭП и регулярное проведение их анализа.

3.4 Запрещается:

- использовать несертифицированные средства квалифицированной ЭП;
- вносить любые изменения в программное обеспечение средств квалифицированной ЭП;
- осуществлять несанкционированное копирование ключей;
- передавать ключевые документы (ключевые носители) лицам, к ним не допущенным, выводить ключевую информацию на печатающие устройства, иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом их использования;
- записывать на ключевые носители постороннюю информацию;
- оставлять СВТ с установленными на них средствами квалифицированной ЭП без контроля после ввода ключевой информации;

– использовать ключ ЭП, связанный с квалифицированным сертификатом ключа проверки ЭП, в отношении которого в аккредитованном удостоверяющем центре Банка России зарегистрировано заявление о прекращении его действия.

## 4 Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной ЭП

4.1 Меры защиты ключей ЭП.

Создаваемые ключи квалифицированной ЭП должны записываться на ключевые носители (далее – КН), имеющее подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности. Не допускается хранение на носителе ключевой информации любой иной информации (в том числе рабочих или личных файлов).

Типы КН, функциональных ключевых носителей (далее – ФКН), которые поддерживаются применяемым средством квалифицированной ЭП, устанавливаются согласно технической и эксплуатационной документации на средство ЭП.

КН, ФКН должны иметь маркировку, обеспечивающую возможность их учёта в организации, использующей средства ЭП.

Ключи квалифицированной ЭП, содержащиеся на КН (ФКН), рекомендуется защищать паролем (ПИН-кодом). При этом лицо, выполняющее процедуру генерации ключей ЭП, обязано сбросить заводской ПИН-код и сформировать новый ПИН-код. В случае, если создание ключа ЭП осуществляется заявителем на средствах аккредитованного удостоверяющего центра Банка России, должны быть приняты меры, исключающие возможность несанкционированного доступа иных лиц к ключу ЭП, записанному на КН (ФКН).

Ответственность за обеспечение конфиденциальности пароля (ПИН-кода) и ключа квалифицированной ЭП возлагается на владельца ключа квалифицированной ЭП.

4.2 Обращение с ключевой информацией и ключевыми носителями.

Запрещается пересылать файлы с ключевой информацией по незащищённым каналам связи (сеть Интернет, корпоративная почта). Данное требование не распространяется на ключи проверки ЭП, содержащиеся в квалифицированном сертификате.

Размещение ключевой информации на локальном диске СВТ или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной ЭП, крайне не рекомендуется, в связи с тем, что создает предпосылки для совершения нарушителями злоумышленных действий.

КН (ФКН) должны использоваться только владельцем ключа ЭП, размещенного на КН (ФКН), и храниться в нерабочие периоды времени в месте, исключающем возможность его бесконтрольного использования. В частности, одним из способов контроля сохранности ключей ЭП, содержащегося на КН (ФКН) является хранение КН (ФКН) в сейфе (металлическом шкафу, колбе), опечатываемом личной печатью владельца ключа ЭП (владельца КН либо ФКН).

В целях минимизации случаев компрометации ключа ЭП, содержащегося на КН (ФКН), рекомендуется вставлять носитель в считывающее устройство только в необходимых случаях, а именно на период выполнения операций формирования и проверки квалифицированной ЭП. В прочее время КН (ФКН) рекомендуется изымать из считывателя в целях исключения риска несанкционированного доступа к КН (ФКН) и его содержимому третьими лицами.

4.3 Обеспечение безопасности СВТ с установленными средствами квалифицированной ЭП.

С целью контроля исходящего и входящего трафика, СВТ с установленными средствами квалифицированной ЭП должны быть защищены от несанкционированного доступа программными или аппаратными средствами.

СВТ, используемые для работы в автоматизированных системах, должны удовлетворять требованиям:

- возможность запуска ОС, входа в систему с использованием парольной защиты, удовлетворяющей требованиям, приведенным в разделе 3 настоящего руководства;
- применение только лицензионного программного обеспечения;
- применение только лицензионных средств антивирусной защиты и регулярно обновляемых антивирусных баз данных (сигнатур);
- отключение всех неиспользуемых служб и процессов, порождаемых ОС, в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.) и включение реально требуемых;
- регулярные обновления ОС, прикладных систем;
- лицам, не имеющим полномочий для работы с СВТ с установленными средствами квалифицированной ЭП, исключен физический доступ к СВТ;
- на СВТ активированы средства регистрации событий информационной безопасности;
- включена автоматическая блокировка СВТ по истечении заданного периода времени неактивности (рекомендуемое время неактивности – не более 10 минут).

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

4.4 Компрометация ключа ЭП.

Под компрометацией ключа ЭП понимается утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации. Компрометация ключей ЭП происходит, как правило, вследствие событий:

- потеря КН (ФКН) либо потеря КН (ФКН) с их последующим обнаружением;
- увольнение работника, имевшего доступ к ключевой информации;
- нарушение целостности печати хранилища КН (ФКН) вследствие несанкционированного вскрытия;
- отсутствие контроля в отношении места нахождения КН (ФКН) в течение неопределенного времени;
- нарушение правил уничтожения ключей ЭП (после окончания срока их действия);
- подозрения на утечку информации или её искажение в системе конфиденциальной связи;
- нарушение работоспособности КН (ФКН) при допущении условия возможных несанкционированных воздействий на носитель;
- другие события утраты доверия к ключевой информации, согласно эксплуатационной документации на используемое СКЗИ.

В первых четырех случаях компрометация ключа ЭП носит явный характер и реагирование в этих случаях должно заключаться в немедленном обращении владельца ключа ЭП в аккредитованный удостоверяющий центр Банка России в целях прекращения действия квалифицированного сертификата.

Прочие случаи должны рассматриваться и анализироваться в каждом конкретном случае. Использование ключа ЭП может быть продолжено только в случаях обоснованной уверенности в сохранении свойств безопасности ключа ЭП.