КОММЕРЧЕСКИЙ БАНК «КУБАНЬ КРЕДИТ»
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
(КБ «КУБАНЬ КРЕДИТ» ООО)

УТВЕРЖДЕН
Правлением КБ «Кубань Кредит» ООО
(Протокол № 1129 от «03» ноября 2022г.)

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

(с учетом Изменений № 1 от 04.10.2024г.)

Зарегистрирован № 513R2(1)

КРАСНОДАР
2022

Содержание

Раздел 1. Введение

1.1. Настоящее «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» (далее – **Руководство**) является средством официального информирования 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.

1.2. Требования настоящего Руководства распространяются на лиц, заинтересованных в получении или владеющих квалифицированным сертификатом ключа проверки ЭП, создаваемым Удостоверяющим центром.

1.3. Владелец сертификата ключа проверки электронной подписи принимает риски, указанные в настоящем Руководстве, связанные с использованием электронных подписей.

1.4. Настоящее Руководство размещается на официальном сайте Банка в информационно-телекоммуникационной сети Интернет по адресу https://kk.ru/.

1.5. При разработке настоящего Руководства использованы следующие нормативные акты и иные документы:

– Федеральный закон от 06.04.2011г. № 63-ФЗ «Об электронной подписи» (далее – **Закон № 63-ФЗ**).

В случае изменения законодательства Российской Федерации, настоящее Руководство до момента его изменения Банком применяется в части, не противоречащей требованиям законодательства Российской Федерации.

1.6. Внутренние нормативные документы Банка в действующей редакции, ссылки на которые приведены в настоящем Руководстве:

– «Порядок реализации функций аккредитованного Удостоверяющего центра КБ «Кубань Кредит» ООО и исполнения его обязанностей» (рег. № 491R).

Раздел 2. Термины, определения и сокращения

2.1. В рамках настоящего Руководства используются следующие термины, определения и сокращения:

Автоматизированное рабочее место (АРМ) – персональный компьютер с программным обеспечением (либо терминал, работающий по технологии тонкого клиента, например VDI, и предоставляющий доступ к удалённо исполняемому ПО) и дополнительными техническими устройствами, необходимыми для выполнения задач, определенных в функциональных обязанностях пользователя.

Банк – коммерческий банк «Кубань Кредит» общество с ограниченной ответственностью (ОГРН 1022300003703, ИНН 2312016641, Генеральная лицензия № 2518 от 03.07.2012г.).

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Информационная система – совокупность информации и обеспечивающих ее обработку информационных технологий и технических средств.

Квалифицированный сертификат ключа проверки ЭП (Квалифицированный сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленными Законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным Удостоверяющим центром либо Федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (уполномоченный федеральный орган), и являющийся в связи с этим официальным документом.

Квалифицированная электронная подпись (КЭП) – электронная подпись, полученная в результате криптографического преобразования информации с использованием

ключа электронной подписи, которая позволяет определить лицо, подписавшее электронный документ, обнаружить факт внесения изменений в электронный документ после момента его подписания, а также создается с использованием средств электронной подписи. Ключ проверки квалифицированной электронной подписи указан в Квалифицированном сертификате. Для создания и проверки такой электронной подписи, используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Законом № 63-ФЗ.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

ОС – операционная система.

ПО – программное обеспечение.

Пользователь УЦ – юридическое, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предприниматель, глава крестьянско-фермерского хозяйства, адвокат, нотариус, арбитражный управляющий и т.п.), который на законных основаниях является владельцем сертификата ключа проверки электронной подписи, выданном Удостоверяющим центром, а также лица, проходящие процедуру получения квалифицированного сертификата ключа проверки ЭП.

Сертификат ключа проверки ЭП (Сертификат) – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной считается действующим если:

– наступил момент времени начала действия сертификата ключа проверки электронной подписи;

– срок действия сертификата ключа проверки электронной подписи не истек;

– сертификат ключа проверки электронной подписи не аннулирован и не прекратил действие.

Система дистанционного банковского обслуживания юридических лиц «iSimple corporate» (система ДБО) – система юридически значимого электронного документооборота, позволяющая клиенту (юридическому лицу/индивидуальному предпринимателю) осуществлять информационное взаимодействие с Банком в режиме удаленного доступа с использованием глобальной информационно-телекоммуникационной сети «Интернет».

Средства электронной подписи (средства ЭП, средства КЭП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) – Банк, осуществляющий функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Законом № 63-ФЗ.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Раздел 3. Условия и порядок использования ЭП и средств ЭП

3.1. Условия и порядок использования ЭП и средств ЭП устанавливаются владельцем информационной системы, в которой пользователь УЦ использует или планирует использовать ЭП и средства ЭП, а также технической и эксплуатационной документацией к средствам ЭП.

3.2. Условия и порядок использования ЭП и средств ЭП в системе ДБО, определяются договором дистанционного банковского обслуживания.

Раздел 4. Риски, связанные с использованием КЭП

4.1. Применение КЭП в государственных и иных информационных системах, а также в системах юридически значимого электронного документооборота, сопровождается, в том числе, следующими рисками:

- финансовые убытки (в том числе штрафы, неустойки и т.п.);
- репутационные риски;
- нарушение сроков оказания государственных, муниципальных и иных услуг;
- нарушение правильного функционирования информационных систем.

4.2. Риски, связанные с применением КЭП, возникают вследствие возможности признания недействительности сделок, совершенных с использованием КЭП, недействительности документов, подписанных КЭП, при несанкционированном получении злоумышленником ключа ЭП или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка КЭП.

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

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

Раздел 5. Требования к организации режима обеспечения безопасности помещений, в которых эксплуатируются средства КЭП

5.1. При эксплуатации средств КЭП 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:

- 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;
- утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в Помещения.

5.2. В случае необходимости присутствия посторонних лиц в Помещениях, должен быть обеспечен контроль за их действиями, во избежание негативных воздействий с их стороны на средства КЭП, средства обработки информации и передаваемую информацию.

5.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в Помещениях должны обеспечивать исполнителям работ сохранность доверенных им документов и сведений, включая ключи ЭП.

Раздел 6. Требования по защите информации от несанкционированного доступа

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

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

– длина пароля должна быть не менее 10 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 (например: «ПО», «ОС» и т.д.) и системные имена (например: «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.

6.1.2. При использовании ключей ЭП, АРМ должны быть сконфигурированы с учетом следующих требований:

– не использовать нестандартные, измененные или отладочные версии ОС;

– исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;

– на АРМ, с установленными средствами ЭП, должна быть установлена только одна ОС;

– все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, службы и т.п.);

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в ОС, 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.

6.1.3. На АРМ необходимо:

– организовать стирание (по окончании сеанса работы средств ЭП) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо – на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

– исключить попадание в систему программ, позволяющих использовать ошибки ОС, для повышения предоставленных привилегий;

– своевременно устанавливать актуальные пакеты обновлений безопасности ОС, своевременно обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

6.1.4. 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 том числе Интернет, без проведения

соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

6.1.5. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых ОС, а также к ПО, 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, организация выделенных сегментов сети и т.п.). В зависимости от технической, конструкторской документации и инструкций, средства защиты могут иметь сертификат уполномоченного органа по сертификации средств защиты.

6.1.6. Необходимо организовать и использовать:

– систему аудита, организовать регулярный анализ результатов аудита;

– комплекс мероприятий по антивирусной защите, с проведением регулярных проверок.

6.2. 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 ПО средств ЭП;

– записывать на ключевые носители постороннюю информацию;

– оставлять АРМ, с установленными средствами ЭП, без контроля после ввода ключевой информации;

– использовать ключ ЭП, связанный с Сертификатом, который аннулирован или действие которого прекращено;

– удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия Сертификата.

– использовать на рабочем месте с ключевой информацией средства обхода функций безопасности ОС и компонентов прикладного ПО.

Раздел 7. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации

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

7.2. Ключи КЭП 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 КЭП.

7.3. Недопустимо пересылать файлы с ключевой информацией по электронной почте, сети Интернет (кроме файлов Квалифицированных сертификатов).

7.4. Ключевую информацию необходимо размещать на отчуждаемом носителе информации (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, существенно повышает риски реализации мошеннических действий.

7.5. 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.).

7.6. Уполномоченное лицо, использующее КЭП, должно назначаться

распорядительным документом по организации, гарантируя возложение обязанностей по работе с КЭП и исполнение правил информационной безопасности.

7.7. Носитель ключевой информации должен подключаться к рабочему месту только на время выполнения средствами ЭП операций формирования и проверки КЭП, шифрования и дешифрования. Подключение носителя ключевой информации к АРМ на продолжительное время, существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

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

Раздел 8. Обеспечение безопасности автоматизированных рабочих мест с установленными средствами ЭП

8.1. С целью контроля исходящего и входящего подозрительного трафика, АРМ 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.

8.2. На технических средствах, используемых для работы в системах обмена электронными документами, необходимо выполнить следующие настройки:

– на учетные записи пользователей ОС должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 5 настоящего Руководства;

– должно быть установлено только лицензионное ПО;

– должно быть установлено лицензионное антивирусное ПО, со своевременно обновляемыми антивирусными базами данных;

– должны быть отключены все неиспользуемые службы и процессы ОС Windows (в том числе службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

– должны своевременно устанавливаться обновления ОС;

– должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами ЭП 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 по простою, более 10 минут с требованием ввода пароля.

8.3. В качестве АРМ, для работы в системах обмена электронными документами, 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.).

8.4. 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.).

Раздел 9. Действия при компрометации ключей КЭП

9.1. К событиям, относящимся к компрометации ключей КЭП, относятся следующие ситуации:

– ознакомление неуполномоченного лица (лиц) с ключами КЭП;

– утрата ключевого носителя с ключами КЭП;

– увольнение пользователя ключа КЭП;

– нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных

для хранения ключевых носителей;

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

– 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);

– вирусное заражение;

– другие случаи, не позволяющие однозначно установить местонахождение ключа или лиц имевших к нему доступ.

9.2. В случае компрометации ключей КЭП. владелец Квалифицированного сертификата должен:

– прекратить использование ключа КЭП и соответствующего Квалифицированного сертификата;

– незамедлительно обратиться в Удостоверяющий центр для аннулирования (прекращения действия) соответствующего Квалифицированного сертификата и получения (при необходимости) нового Квалифицированного сертификата в соответствии с «Порядком реализации функций аккредитованного Удостоверяющего центра КБ «Кубань Кредит» ООО и исполнения его обязанностей» (в действующей редакции, размещенной на сайте kk.ru).

Раздел 10. Заключительные положения

10.1. Настоящее Руководство утверждается Правлением Банка и вводится в действие с 09 ноября 2022 года.

10.2. С даты ввода в действие настоящего Руководства, утрачивает силу «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» рег. № 513R1 (утвержден: Правлением Банка, Протокол № 780 от «29» июня 2018г.).