«УТВЕРЖДАЮ»
Директор АО «КАЛУГА АСТРАЛ»
_____ И.И. Чернин
«29» 05 2025 г.

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

1. Введение

Настоящее Руководство предназначено для обязательного ознакомления Пользователя Удостоверяющего центра АО «КАЛУГА АСТРАЛ» (далее – Пользователь УЦ), использующего квалифицированную электронную подпись и средство(а) квалифицированной электронной подписи.

2. Определения

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.

Сертификат ключа проверки электронной подписи - 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.

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – ФЗ № 63) 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.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном ФЗ № 63 порядке выдан сертификат ключа проверки электронной подписи.

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

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

Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные ФЗ № 63.

Средства электронной подписи - 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.

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

3. Работа со средствами электронной подписи (ЭП)

Пользователи Удостоверяющего центра АО «КАЛУГА АСТРАЛ», осуществляющие работу со средствами электронной подписи, получившие и использующие ключи электронной подписи, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы со средствами ЭП;
- сохранение в тайне содержания средств ЭП;
- сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;
- сохранение в тайне пин-кодов для доступа к носителям ключевой информации и средствам ЭП;
- самостоятельное удаление информации с носителя ключевой информации;
- самостоятельное проведение инициализации носителя ключевой информации, повлекшее удаление информации с носителя ключевой информации;
- своевременную подачу заявления на прекращение действия сертификата ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи нарушена (см. п. 5 настоящего Руководства - «Компрометация ключей»);
- своевременное обновление сертификата ключа проверки электронной подписи при истечении его срока действия (плановую смену).

Срок действия квалифицированного сертификата, создаваемого Удостоверяющим центром АО «КАЛУГА АСТРАЛ» для Пользователя УЦ, указывается в сертификате ключа проверки электронной подписи и не может быть более срока, определенного требованиями, установленными эксплуатационной документацией на средства электронной подписи и средства Удостоверяющего центра, прошедшими в установленном порядке процедуру соответствия требованиям, установленным в соответствии с ч. 5 ст. 8 ФЗ № 63, с использованием которых такой сертификат ключа проверки электронной подписи создается. Заблаговременно до истечения этого срока владелец сертификата ключа проверки электронной подписи, если же в этом есть необходимость, обязан заменить его, обратившись в Удостоверяющий центр АО «КАЛУГА АСТРАЛ».

Пользователями УЦ должны быть обеспечены соответствующие условия хранения носителей ключевой информации, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования средств ЭП.

Пользователь УЦ также несет ответственность за то, чтобы на компьютере, на котором установлены средства ЭП, не были установлены и не эксплуатировались программы (в том числе вирусы), которые могут нарушить функционирование программных средств и средств ЭП.

При обнаружении на рабочем месте, оборудованном средствами ЭП, 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.

Не допускается:

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить информацию о средствах ЭП на дисплей и принтер;
- подсоединять носитель ключевой информации к компьютеру при проведении работ, не являющихся штатными процедурами использования средств ЭП (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи);

- вносить какие-либо изменения в программное обеспечение и средства ЭП;
- осуществлять несанкционированное копирование ключевой информации с носителя ключевой информации;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами квалифицированной ЭП без контроля после ввода ключевой информации;
- использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена (см. п. 5 настоящего Руководства - «Компрометация ключей»);
- использовать ключ электронной подписи и соответствующий сертификат, заявление на прекращение действия которого подано в удостоверяющий центр;
- использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено;
- пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме ключей проверки ЭП);
- использовать несертифицированные в соответствии законодательством Российской Федерации средства ЭП.

4. Рекомендуемые организационно-технические меры по обеспечению информационной безопасности в организации

Для хранения электронных ключей и средств ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).

Использовать автоматизированное рабочее место (АРМ) с установленными средствами ЭП необходимо в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 8 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка операционной системы (ОС) без запроса пароля. При этом должны быть реализованы дополнительные организационно-режимные меры, исключающие несанкционированный доступ к этим АРМ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ с установленными средствами ЭП.

Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами ЭП.

Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

Администрирование должно осуществляться доверенными лицами.

Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 8 символов.

После получения носителя ключевой информации в точке выдачи АО «КАЛУГА АСТРАЛ» рекомендуется произвести смену стандартного пин–кода носителя ключевой информации на свой собственный. Длина пароля должна быть не менее 8 символов.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям, должна быть проведена смена ключей электронной подписи, к которым он имел доступ.

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

На технических средствах, используемых для работы в информационных системах:

- 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 (в том числе службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски);
- должны регулярно устанавливаться обновления операционной системы;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

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 владельцу сертификата, в том числе средства ЭП, журналы работы систем обмена электронными документами.

5. Компрометация ключей

Под компрометацией ключей электронной подписи понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к носителям ключевой информации или к ключевой информации на данных носителях, любые другие виды разглашения информации о средствах ЭП, в результате которых средства ЭП могут стать доступными несанкционированным лицам и (или) процессам.

Пользователь Удостоверяющего центра должен самостоятельно определить факт компрометации ключа электронной подписи и оценить значение этого события. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием средств ЭП, организует и осуществляет сам Пользователь УЦ.

В случае компрометации владелец ключа электронной подписи (Пользователь УЦ) обязан незамедлительно обратиться в Удостоверяющий центр АО «КАЛУГА АСТРАЛ» с заявлением на прекращение действия сертификата ключа проверки электронной подписи.

6. Заключение

Настоящее Руководство составлено на основании:

- Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказа ФАПСИ от 13.06.2001 № 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»;

- Приказа ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».