«УТВЕРЖДАЮ»
Генеральный директор ООО «АСТРАЛ-М»
_____Ю.Н. Мео
«09» января 2019 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 ООО «АСТРАЛ-М», использующего квалифицированную электронную подпись и средство(а) квалифицированной электронной подписи.

2. Определения

Система - автоматизированная информационная система передачи и приема информации в электронном виде по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием средств электронной подписи.

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 законом 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, а также граждане.

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Электронные ключи – персональное средство аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью.

3. Работа со средствами электронной подписи (ЭП)

Пользователи Удостоверяющего центра ООО «АСТРАЛ-М», 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 электронным ключам и средствам ЭП;
- самостоятельное удаление информации с электронного ключа;
- самостоятельное проведение инициализации электронного ключа, повлекшее удаление информации с электронного ключа;
- 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 ключа»);
- своевременное обновление сертификата ключа проверки электронной подписи при истечении его срока действия (плановую смену).

Срок действия сертификата ключа проверки электронной подписи – один год с момента изготовления. Заблаговременно до истечения этого срока владелец сертификата ключа проверки электронной подписи, если же в этом есть необходимость, обязан заменить его, обратившись в любую Точку выдачи аккредитованного Удостоверяющего центра ООО «АСТРАЛ-М». Адреса Точек выдачи можно найти на сайте ООО «АСТРАЛ-М» https://astral.ru/

Пользователями УЦ должны быть обеспечены соответствующие условия хранения электронных ключей, 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 электронных носителей или передавать сами носители лицам, к ним не допущенным, выводить информацию о средствах ЭП на дисплей и принтер;
- подсоединять электронный носитель к USB – порту компьютера 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), а также в USB – порты других ПК;
- вносить какие – либо изменения в программное обеспечение и средства ЭП;
- осуществлять несанкционированное копирование ключевой информации с электронного ключа.

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 6 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 6 символов.

После получения электронного ключа в точке выдачи ООО «АСТРАЛ-М» рекомендуется произвести смену стандартного пин – кода электронного ключа на свой собственный. Длина пароля должна быть не менее 6 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.

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 ключевым носителям 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 любую Точку выдачи аккредитованного Удостоверяющего центра ООО «АСТРАЛ-М» с заявлением на прекращение действия сертификата ключа проверки электронной подписи по факту компрометации ключа электронной подписи (бланк заявления на прекращение действия сертификата размещен в Регламенте УЦ на сайте https://ca.astralm.ru/, так же его можно взять в Точке выдачи у Доверенного лица Удостоверяющего центра.

Прекращение действия сертификата ключа проверки электронной подписи производится только при личном прибытии владельца сертификата ключа проверки электронной подписи в Точку выдачи и предъявлению основного документа удостоверяющего личность – паспорта.

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