«УТВЕРЖДАЮ»
Директор ООО «АСТРАЛ-СОФТ»

_____И.И. Чернин
«11» ноября 2022 г.

Руководство

по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи

1. Введение

Настоящее руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи (далее – Руководство) предназначено для обязательного ознакомления пользователя удостоверяющего центра ООО «Астрал-Софт» (далее – Пользователь), использующего неквалифицированную электронную подпись и средство(а) 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.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом от 06.04.2011 № 63 – ФЗ «Об электронной подписи» (далее – 63-ФЗ) 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 (УЦ) - 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.

Для целей настоящего Руководства под Удостоверяющим центром понимается ООО «Астрал-Софт».

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.

3. Работа со средствами электронной подписи (ЭП)

Пользователи Удостоверяющего центра, осуществляющие работу с электронной подписью, получившие и использующие средства доступа к 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;
- сохранение в тайне паролей/пин – кодов для доступа к устройствам и средствам ЭП;
- 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 Удостоверяющего центра .

Пользователями УЦ должны быть обеспечены соответствующие условия хранения средств доступа к ЭП, исключающие возможность доступа к ним посторонних лиц и несанкционированного их использования.

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

При обнаружении на устройстве посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном устройстве должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

4. Рекомендуемые организационно – технические меры по обеспечению информационной безопасности

После получения средств для настройки и активации ЭП в точке выдачи Удостоверяющего центра, должны быть предусмотрены меры, исключающие возможность несанкционированного доступа к ним третьих лиц.

Использовать устройство с установленными средствами доступа к ЭП необходимо в однопользовательском режиме.

Должны быть приняты меры по исключению несанкционированного доступа к устройствам со средствами доступа к ЭП.

5. Компрометация ключа электронной подписи

Под компрометацией ключа электронной подписи понимается утрата устройств с настроенными и активированными средствами доступа к электронной подписи (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 устройствам или к ключевой информации на данных устройствах, 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 ключа владелец электронной подписи (Пользователь УЦ) обязан незамедлительно обратиться в любую точку выдачи Удостоверяющего центра с заявлением на прекращение действия сертификата ключа проверки электронной подписи по факту компрометации ключа электронной подписи в соответствии с процедурой, установленной Порядком реализации функций удостоверяющего центра ООО «АСТРАЛ-СОФТ» по созданию и выдаче сертификатов ключей проверки усиленной неквалифицированной электронной подписи (далее - Регламент). Бланк заявления на прекращение действия сертификата размещен в Регламенте, на сайте УЦ по ссылке: http://as.keydisk.ru/, а так же его можно получить в точке выдачи у доверенного лица Удостоверяющего центра.

6. Нормативно-правовая база

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)».