ИНФОРМАЦИОННЫЙ ОПЕРАТОР SZTLS ООО «СЕВЕРО-ЗАПАДНЫЙ ТАМОЖЕННО-ЛОГИСТИЧЕСКИЙ СЕРВИС»

РУКОВОДСТВО ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СРЕДСТВ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

При использовании электронной подписи (далее – ЭП) существуют риски, связанные с раскрытием информации о ключе ЭП, с несанкционированным доступом (далее – НСД) к средствам ЭП:

- возможность несанкционированного совершения юридически значимых действий от имени владельца квалифицированного сертификата ключа проверки ЭП (далее – КСКПЭП);
- возможность внесения несанкционированных изменений в электронный документооборот.

Безопасность использования квалифицированной ЭП и средств ЭП обеспечивается соблюдением комплекса правовых, организационных и технических мер. В целях обеспечения безопасности использования квалифицированных ЭП и средств ЭП необходимо:

- назначить в организации должностных лиц, ответственных за обеспечение информационной безопасности и эксплуатацию средств ЭП;
- разработать и ввести в организации в действие организационно-распорядительные документы, регламентирующие вопросы безопасности использования средств ЭП;
- соблюдать порядок использования и хранения носителей ключевой информации ЭП, исключающего возможность НСД к ключевой информации ЭП;
- принять меры, исключающие возможность НСД к средствам ЭП;
- вести поэкземплярный учет носителей ключевой информации ЭП, средств ЭП, эксплуатационной и технической документации к ним в выделенных для этих целей журналах.

Квалифицированная ЭП может использоваться при соблюдении следующих условий: КСКПЭП создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата; КСКПЭП действителен на момент подписания электронного документа; квалифицированная ЭП используется с учетом ограничений, содержащихся в КСКПЭП, если такие ограничения установлены.

Владелец КСКПЭП обязан:

- обеспечивать конфиденциальность ключей ЭП, в частности не допускать использования принадлежащих ему ключей ЭП без его согласия;
- не использовать ключ ЭП и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший КСКПЭП, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена;
- уведомить иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- использовать для создания и проверки квалифицированных ЭП средства ЭП, получившие подтверждение соответствия требованиям, установленным законодательством РФ.

Порядок использования и хранения носителей ключевой информации ЭП должен исключать возможность НСД к ключевой информации ЭП. Не допускается:

- снимать несанкционированные копии с ключевых носителей ЭП;
- передавать ключевые носители и/или ознакомлять с содержанием носителей ключевой информации ЭП лиц, не являющихся владельцами КСКПЭП, связанных с ключами, находящимися на данных носителях;

- выводить ключи ЭП на дисплей (монитор) автоматизированного рабочего места автоматизированной системы со средствами ЭП (далее – АРМ АС) или принтер;

- записывать на ключевой носитель ЭП постороннюю информацию.

Рекомендуется после получения ключевого носителя ЭП сменить пароль доступа (PIN-код) к ключевому контейнеру и обеспечить конфиденциальность его хранения. Рекомендуется использовать носители ключевой информации ЭП только непосредственно при работе с системами электронного документооборота в моменты выполнения операций подписания. По завершении операций необходимо извлечь ключевой носитель из считывающего устройства. Для хранения носителей ключей ЭП необходимо выделить надежно запираемый сейф или иное хранилище, оборудованные приспособлением для опечатывания, а также принимать другие меры, исключающие НСД к носителям ключевой информации ЭП. При транспортировке носителей ключевой информации ЭП необходимо создать условия, обеспечивающие их защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Для создания и проверки квалифицированной ЭП должны использоваться средства ЭП, которые позволяют установить факт изменения подписанного электронного документа после его подписания, обеспечивают практическую невозможность вычисления ключа ЭП из ЭП или из ключа ее проверки. При создании квалифицированной ЭП средства ЭП должны:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

- создавать квалифицированную ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию квалифицированной ЭП;

- однозначно показывать, что квалифицированная ЭП создана.

При проверке квалифицированной ЭП средства ЭП должны:

- показывать содержание электронного документа, подписанного квалифицированной ЭП;

- показывать информацию о внесении изменений в подписанный квалифицированной ЭП электронный документ;

- указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Средства ЭП, предназначенные для создания квалифицированных ЭП в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации. Для создания и проверки квалифицированной ЭП должны использоваться средства ЭП, получившие подтверждение соответствия требованиям, установленным законодательством РФ.

Установка и настройка средств ЭП на АРМ АС должна выполняться лицами, имеющими соответствующий уровень подготовки. Перед установкой необходимо проверить целостность программного обеспечения (далее – ПО) средств ЭП. Запрещается устанавливать ПО средств ЭП, целостность которого нарушена. ПО средств ЭП следует устанавливать на АРМ с предустановленными и настроенными сертифицированными в соответствии с правилами сертификации РФ средствами защиты информации (программными и/или программно-аппаратными) – антивирусными программными средствами, комплексами средств защиты информации от НСД, межсетевыми экранами, средствами анализа защищенности и средствами обнаружения вторжений.

Средства ЭП должны использоваться в соответствии с положениями эксплуатационной документации на применяемое средство ЭП.

При использовании средств ЭП необходимо:

- исключить возможность НСД лиц к АРМ с установленными средствами ЭП;

- исключить несанкционированную модификацию средств ЭП;

- приступать к применению средств ЭП только после изучения эксплуатационной документации по их использованию.

Доступ в помещения, в которых размещаются АРМ АС, должен быть ограничен и исключена возможность бесконтрольного проникновения в них посторонних лиц. Размещение оборудования АРМ АС должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности. Размещение технических средств АРМ АС в помещении должно исключать возможность визуального просмотра экранов мониторов через окна. Рекомендуется сформировать с помощью комплекса средств защиты информации от НСД функционально замкнутую среду, обеспечивающую контроль целостности ПО и допускающую работу пользователей строго в рамках предоставляемых им возможностей и полномочий. Защите подлежат системные и загрузочные файлы, а также файлы, связанные с работой средств ЭП. На АРМ АС не должны устанавливаться средства разработки ПО и отладчики. Рекомендуется полностью блокировать сетевой доступ к ресурсам АРМ АС (в том числе удаленный вход в сеть) с других АРМ локальной сети и в особенности из внешних сетей, или по крайней мере ограничить список доступных для соединения адресов. С этой целью рекомендуется установить и настроить соответствующим образом межсетевой экран. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное ПО. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов.

Пользователи АРМ АС не должны иметь администраторских прав с целью ограничения возможностей установки под этими учетными записями ПО на АРМ АС. Доступ к файловым ресурсам АРМ АС, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены. Пользователи АРМ АС обязательно должны быть проинструктированы по вопросам соблюдения основных требований информационной безопасности, и в особенности по вопросам использования антивирусных программ и средств ЭП. Локальными (или доменными) политиками на АРМ АС рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему (далее – ОС) АРМ АС. Рекомендуется ограничить или полностью отказаться от приема внешней (из международной ассоциации сетей Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами. На АРМ АС должна быть установлена только одна ОС. Средствами BIOS АРМ АС следует исключить возможность загрузки ОС, отличной от установленной на жестком диске. Доступ к изменению настроек BIOS должен быть защищен паролем. При загрузке ОС и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль. Пользователям должны быть назначены данные пароли. Длина паролей должна составлять не менее восьми символов. Срок действия паролей должен быть ограничен. Пароли должны учитываться, обновляться и храниться в соответствии с порядком, установленным в организации. Хранение списков паролей, инсталляционных дисков с ПО средств ЭП и документации к таким средствам должно осуществляться в надежно запираемом хранилище, оборудованном приспособлением для опечатывания, с принятием комплекса мер, исключающих НСД к упомянутой информации.

Рекомендуется опечатать системный блок АРМ АС для предотвращения его несанкционированного вскрытия. Для ограничения доступа к АРМ АС, проверки целостности используемого ПО рекомендуется устанавливать комплексы средств защиты информации от НСД. Рекомендуется произвести аттестацию АС по требованиям безопасности информации. Не рекомендуется подключать к АРМ АС внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.