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

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Введение**

Настоящее руководство предназначено для обязательного ознакомления Пользователя Удостоверяющего центра ЗАО «ЦЭК», использующего средства электронной подписи (ЭП).

1. **Общие положения и определения**

***Система -*** автоматизированная информационная система передачи и приемаинформации 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,котораяприсоединена 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 илидокумент 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, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

***Владелец сертификата ключа проверки электронной подписи*** -лицо,которому вустановленном настоящим Федеральным 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 (далее - проверка электронной подписи);

***Удостоверяющий центр*** -юридическое лицо или индивидуальныйпредприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

***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 информациейв 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 защищённогохранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью.

1. **Работа со средствами электронной подписи (ЭП)**

Пользователи Удостоверяющего центра ЗАО «ЦЭК», 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 повторной инициализации электронного ключа, повлекшее удаление информации с электронного ключа;
* своевременную подачу заявления о приостановлении действия или аннулировании 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 (плановая смена).

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 ЗАО «ЦЭК». Адреса точек выдачи можно найти на сайте ЗАО «ЦЭК» [http:\\www.cek.ru](http://www.cek.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 так же 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;
1. **Риски использования электронной подписи**

При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

* Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.
* Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.
* Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.
* Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.
* Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избежания помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

1. **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 ЗАО «ЦЭК» 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.

1. **Компрометация ключа**

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 точку выдачи ЗАО «ЦЭК», производившую выпуск ключа электронной подписи, с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи по факту компрометации ключа электронной подписи (бланк заявления можно взять в точке выдачи или на сайте [http:\\www.cek.ru](http://www.cek.ru)).

**Аннулирование (отзыв) сертификата ключа проверки электронной подписи производится только при личном прибытии владельца сертификата ключа проверки электронной подписи в точку выдачи и предъявлению документа, удостоверяющего личность – паспорта.**

1. **Заключение**

Настоящее Руководство составлено на основании:

* Федерального закона от 10.01.2002 № 1 – ФЗ «Об электронной цифровой подписи»;
* 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)».