*Приложение № 21*

*к Порядку Удостоверяющего Центра*

*АО «Холдинговая компания Гарант»*

**Правила**

**использования средств криптографической защиты информации и электронной подписи**

1. Средства электронной подписи - шифровальные (криптографические) средства (СКЗИ), используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа проверки, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 г. 63-ФЗ «Об электронной подписи» СКЗИ и средства электронной подписи могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.
2. Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.
3. Для работы с СКЗИ и ключами электронной подписи привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Данные должностные лица, уполномоченные соответствующим приказом руководителя организации, несут персональную ответственность за:
4. Сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
5. Сохранение в тайне содержания ключей электронной подписи;
6. Сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.
7. В организации должны быть обеспечены условия хранения ключевых носителей ключей электронной подписи, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.
8. Уполномоченные лица несут ответственность за то, чтобы на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, 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.
9. Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 года № 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». Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению обладателем конфиденциальной информацией на месте, путем переформатирования ключевых носителей средствами ПО СКЗИ.
10. Не допускается:
11. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;
12. Вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;
13. Записывать на ключевом носителе постороннюю информацию;
14. Вносить какие-либо изменения в СКЗИ и ключ электронной подписи;
15. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).
16. Действия в случае компрометации ключей:
17. 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 ключевой информации, в результате которых ключи электронной подписи могут стать доступными несанкционированным лицам и (или) процессам.
18. Владелец ключа электронной подписи (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа электронной подписи и оценить значение этого события. Мероприятия по локализации последствий компрометации ключей электронной подписи организует и осуществляет сам владелец.
19. При компрометации ключа электронной подписи, владелец ключа должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации (контактная информация размещена на сайте http://www.hkgarant.ru/). Заявление на аннулирование сертификата может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя УЦ в офис удостоверяющего центра, либо почтовой или курьерской доставкой, а также в электронной форме, подписанное усиленной квалифицированной электронной подписью не позднее 12 часов после поступления заявления на аннулирование ключа электронной подписи, сертификат проверки ключа электронной подписи будет отозван. Последующая разблокировка аннулированного сертификата ключа проверки электронной подписи не возможна.

Для получения новых ключей уполномоченный представитель организации, у которой были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, необходимые для выпуска нового ключа электронной подписи. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.

С правилами ознакомлен \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, наименование организации, Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Генеральный директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/