Удостоверяющий центр АО «ЦентрИнформ»

Руководство
по обеспечению безопасности использования электронной подписи и средств электронной подписи

Для обеспечения информационной безопасности при работе с ключами и средствами электронной подписи пользователь владелец ключа электронной подписи обязан строго придерживаться следующих требований и рекомендаций:

Владелец ключа электронной подписи обязан:

- Хранить в тайне ключи электронной подписи.
- Немедленно сообщать Удостоверяющему центру о факте и требовать аннулирования сертификата ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи нарушена (компрометация ключа).

К компрометации ключей можно отнести следующие события: утрата ключевого носителя (в том числе с последующим обнаружением); хищение; несанкционированное копирование; передача ключевой информации по каналам связи в открытом виде; *увольнение сотрудников, имевших доступ к ключевой информации;* любые другие виды разглашения ключевой информации, в результате которых ключи могут стать доступны лицам, к ним не допущенным.

- Обновлять сертификат ключа проверки электронной подписи в соответствии с установленным регламентом Удостоверяющего центра.

Настоятельно рекомендуется:

- Для хранения носителей ключевой информации в помещениях использовать надежные хранилища (например, сейфы), оборудованные надежными запирающими устройствами. Режим хранения должен исключать возможность несанкционированного доступа к ним.
- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средствами электронной подписи, посторонних лиц.
- Для исключения утраты ключевой информации вследствие дефектов носителя рекомендуется использовать дополнительный носитель для создания резервной копии ключевой информации.
- Расположение рабочего места в помещении должно обеспечивать, сохранность конфиденциальных документов и сведений, выводимых на экран.
- На рабочем месте должно быть установлено и регулярно обновляться антивирусное программное обеспечение.
- Предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочего места с установленными средствами электронной подписи, например опечатывание.
- При загрузке операционной системы (ОС) 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 ОС без запроса пароля. При этом должны быть реализованы дополнительные меры, исключающие несанкционированный доступ к этому рабочему месту.
- Установленное на рабочее место программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
- Администрирование программного обеспечения должно осуществляться доверенными лицами.

Не допускается:

- Разглашать содержимое носителей ключевой информации, выводить ключевую информацию на дисплей и принтер.
- Передавать пароли и сами носители ключевой информации лицам, к ним не допущенным.
- Записывать на ключевой носитель постороннюю информацию.
- Использовать ключевые носители, не предусмотренные эксплуатационной документацией на средства электронной подписи.
- Вносить какие-либо изменения в программное обеспечение средств электронной подписи.