**Инструкция по безопасности использования электронной подписи и средств электронной подписи на рабочем месте.**

Порядок обеспечения информационной безопасности при работе в рамках информационной системы, предполагает выполнение пользователем некоторых рекомендаций при использования электронной подписи и средств электронной подписи на рабочем месте:

**Владелец сертификата электронной подписи обязан:**

* Хранить в тайне ключи электронной подписи;
* Немедленно 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.

**Рекомендуется:**

* Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения носителей с ключевой информации, создать резервные копии.
* Для хранения носителей ключевой информации в помещениях рекомендуется устанавливать 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 СКЗИ, посторонних лиц.
* Расположение рабочего места в помещении должно обеспечивать, сохранность конфиденциальных документов и сведений, выводимых на экран.
* На рабочем месте должно быть установлено антивирусное программное обеспечение.
* Рекомендуется предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочего места с установленными СКЗИ, 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 в режимах, не предусмотренных их функционированием.
* Вносить какие-либо изменения в программное обеспечение СКЗИ.