Памятка пользователю
по обеспечению безопасности при использовании квалифицированной электронной подписи и средств электронной подписи

1. **Не доверяйте** Ваш компьютер для обслуживания **посторонним лицам**, исключите **бесконтрольный** доступ в помещения, в которых размещаются средства ЭП.

2. **Не передавайте никому личный ключевой носитель и не сообщайте PIN-код доступа к нему кому бы то ни было!** Доступ к ключевым носителям должен быть только у их владельцев! **Категорически запрещается оставлять личный ключевой носитель и\или PIN-код доступа к нему без присмотра!**

3. Работайте под учетной записью обычного пользователя (**без прав администратора) с надежным паролем** (от 8 символов).

4. **Не отключайте антивирусное программное обеспечение**, настройте регулярное обновление антивирусных баз, установите **максимальный уровень безопасности параметров сетевой защиты (при работе через Интернет)** и **включите защиту паролем на изменение настроек.**

5. Будьте очень осторожны при получении сообщений с **файлами-вложениями.** Обращайте внимание на **расширение файла**. Вредоносные файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того чтобы видеть настоящее расширение файла, обязательно включите в системе **режим отображения расширений файлов.** Проводите **полную еженедельную проверку** компьютера на наличие вирусов.

6. В случае необходимости доступа в информационно-телекоммуникационную сеть «Интернет», установите и настройте на компьютере **персональный межсетевой экран**, разрешив доступ только к доверенным ресурсам сети «Интернет».

7. Для предотвращения удаленного управления Вашим компьютером злоумышленниками не допускайте установки кем бы то ни было на компьютер **программ удаленного администрирования**. Периодически контролируйте установленное и запущенное (работающее) на компьютере ПО.

8. **Блокируйте** компьютер при уходе с рабочего места, при длительном отсутствии – **обязательно выключайте** компьютер.

9. Если Вы работаете **на ноутбуке (переносном компьютере), не храните его вместе со всеми атрибутами доступа** (**личный ключевой носитель**, PIN-коды к нему, логин и пароль).

10. В случае **утраты** личного ключевого носителя или PIN-кода доступа к нему для блокировки использования Вашего ключа подписи посторонними лицами немедленно известите Удостоверяющий центр о нарушении конфиденциальности **ключа ЭП**.

11. **ЗАПРЕЩАЕТСЯ** устанавливать режим **«Включить кэширование»** в настройках режима работы криптопровайдера. Кэширование заключается в том, что считанные с ключевого носителя ключи останутся загруженными в памяти службы хранения ключей и будут доступны любому приложению после извлечения ключевого носителя из считывателя и до завершения работы компьютера. Это означает, что в случае хакерской атаки на Ваш компьютер, злоумышленник сможет воспользоваться загруженными ключами для выработки ЭП от Вашего имени.

12. Если вам в течение сеанса работы со средствами ЭП приходится многократно

использовать ключевой носитель, то для ускорения работы используйте настройку криптопровайдера «Запомнить пароль». После завершения сеанса работы обязательно удалите запомненные пароли, для чего используйте возможности криптопровайдера.