Руководство по обеспечению безопасности использования электронной подписи, средств электронной подписи, ключевого носителя многократного использования.

Основные риски при использовании электронной подписи (далее – ЭП) связаны с несанкционированным доступом к ключам ЭП (т.е. использованием без ведома их владельца), вследствие чего становится возможным возникновение электронных документов, порождающих нежелательные юридически значимые последствия в отношении владельца сертификата ЭП. Источниками несанкционированного доступа могут быть как преднамеренные либо неумышленные действия человека, так и активность вредоносного программного обеспечения.

Далее приводится краткий перечень основных мер безопасности для владельцев ЭП, направленных на избежание указанных рисков.

Исключить пребывание посторонних лиц в помещениях с ключами и средствами ЭП, их доступ к рабочему месту, либо, в случае необходимости пребывания, обеспечить контроль над их действиями.

Обеспечить режим обращения с ключевыми носителями при использовании и хранении, исключающий возможность несанкционированного доступа к ним.

Использовать на рабочем месте лицензионное программное обеспечение (далее – ПО) стабильных версий, полученное из вызывающих доверие источников. Не использовать измененные, взломанные или неподдерживаемые производителем версии ПО.

Использовать на рабочих местах антивирусное ПО.

Использовать на рабочих местах средства межсетевого экранирования (firewall) с определением правил доступа к сетевым ресурсам. Установить и использовать средство ЭП строго в соответствии с эксплуатационной документацией.

Регулярно отслеживать и устанавливать обновления безопасности для ПО, обновлять антивирусные базы.

Использовать политику назначения и смены паролей (на вход в операционную систему, параметры BIOS, экранную заставку и т.д.) в соответствии с общепринятыми рекомендациями по созданию сильных паролей. При покидании рабочего места с активным сеансом пользователя блокировать его паролем.

При наличии оснований полагать, что конфиденциальность ключа ЭП нарушена (произошла компрометация ключа), немедленно принять меры по прекращению действия сертификата ЭП:

- подать заявку на блокировку через Каталог ИТ-услуг в категории ***Безопасность › Информационная безопасность › Криптографическая защита › Работа с токеном (пин-код, поломка, утеря) › Заблокировать при утере.***
- при недоступности Каталога ИТ-услуг сообщить об инциденте в Службу поддержки пользователей группы компаний «Северсталь» по телефону : 8-800-444-09-90 или e-mail: help@severstal.com.

К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей, в том числе с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения ключевых носителей;
- возникновение подозрений на утечку информации.

Не использовать для создания ЭП ключи, если известно, что эти ключи используются или использовались ранее лицами, не имеющими доступа к ним.