Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Термины и определения:

электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

владелец квалифицированного сертификата ключа проверки электронной подписи (далее - владелец сертификата) — лицо, которому в установленном порядке выдан квалифицированный сертификат ключа проверки электронной подписи.

квалифицированный сертификат ключа проверки электронной подписи (далее - сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата.

средства электронной подписи — программные обеспечения, используемые при формировании электронной подписи и рекомендованные удостоверяющим центром (в частности: драйвер на отчуждаемый ключевой носитель Rutoken Driver, криптопровайдер ViPNet CSP, программное обеспечение ViPNet PKI Client).

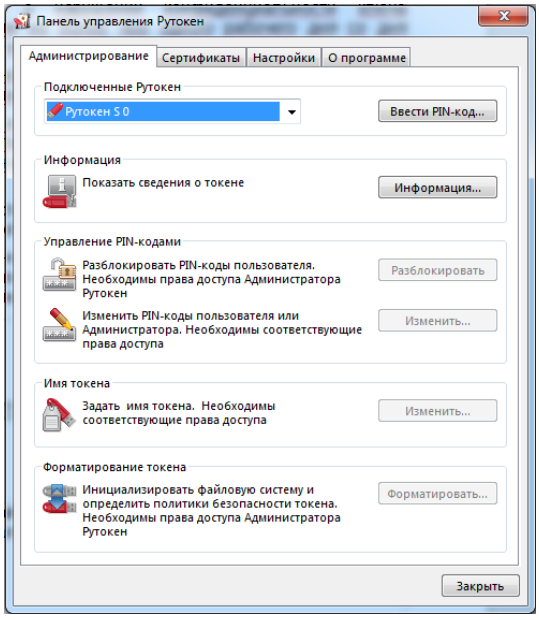
При использовании квалифицированной электронной подписи владельцу необходимо:

1) хранить в тайне (обеспечить конфиденциальность) ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и (или) несанкционированного использования, в частности не допускать использование ключа электронной подписи без своего согласия;
2) уведомлять удостоверяющий центр, выдавший сертификат, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
4) использовать средства электронной подписи, рекомендованные удостоверяющим центром;
5) при нарушении работы средств электронной подписи уведомлять об этом ответственных за их работоспособность лиц или удостоверяющий центр.

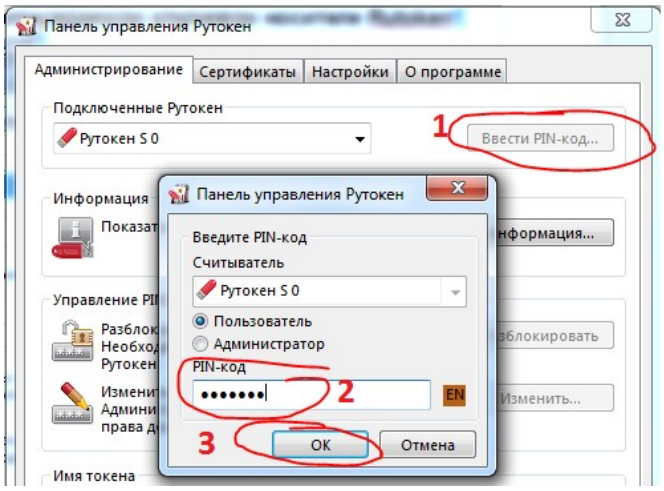
Если сертификат выдан на должностное лицо, выступающего от имени юридического лица, то при увольнении или смене полномочий должностного лица юридическому лицу необходимо аннулировать его сертификат, обратившись в удостоверяющий центр.

Инструкция смены PIN-кода на отчуждаемом ключевом носителе Rutoken

Открыть программу Rutoken Control Panel



Ввести PIN-код, установленный ранее или установленный удостоверяющим центром при генерации ключей электронной подписи (сообщается при передаче ключевого носителя)



Изменить PIN-код пользователя