

Эксперты информационной безопасности Кадастровой палаты по Самарской области подчёркивают главное: если мошенник получил доступ к чужой электронной подписи, то спектр его действий от имени другого человека становится неограниченным.

Поэтому правило № 1: беречь от посторонних посягательств носитель, на котором хранится информация для создания электронной подписи. При получении квалифицированного сертификата электронной подписи важно установить надежный PIN-код к хранилищу ключевой информации и держать пароль в тайне. Если возникло подозрение, что конфиденциальность ключевой информации была нарушена, надо незамедлительно обратиться в аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат подписи, чтобы приостановить или прекратить его действие.

Надо понимать, что самой электронной подписью завладеть нельзя, речь идёт о возможных посягательствах на инструмент для создания подписи от чьего-либо имени. Таким инструментом служит так называемый закрытый ключ электронной подписи – это конфиденциальная информация владельца сертификата электронной подписи. В совокупности сертификат подписи и соответствующий ему закрытый ключ являются аналогом личной подписи гражданина, а для юридических лиц аналогом подписи руководителя и печати. Доступ посторонних лиц к закрытому ключу электронной подписи является несанкционированным.



