***Как избежать мошенничества с электронной подписью***

 По данным [Федеральной службы государственной регистрации, кадастра и картографии от 14 июня 2019 г.](http://internet.garant.ru/#/document/72270924/entry/0) любой владелец недвижимого имущества может подать заявление о том, что сделки с принадлежащим ему имуществом могут производиться только при его личном участии. При подаче такого заявления в Единый государственный реестр недвижимости (ЕГРН) будет внесена соответствующая запись.

 Варианты мошенничества с электронной подписью:
 1) Физические преступления — для развертывания мошеннической схемы необходим контакт преступника с носителем.
 1.1. Кража носителя — простая, как 5 копеек, схема, когда преступник похищает usb-токен, что позволяет ему свободно использовать чужую электронную подпись.

Нейтрализация: — установка пользовательского пароля — напомним, что носители выпускаются со стандартными заводскими паролями, которые находятся в свободном доступе в интернете и, соответственно, их важно заменить на числовую комбинацию, известную только владельцу. После 3 попыток злоумышленника подобрать пароль, usb-токен заблокируется.

 1.2. Добровольная передача своей ЭП другому лицу — исходя из безграничного доверия, а скорее всего из-за непонимания возможных последствий, уполномоченные лица вместо делегирования прав совершать определенные действия передают подчиненным свою электронную подпись.

 **Нейтрализация:** — никогда, никому и ни при каких обстоятельствах не передавать свою электронную подпись — наверное, самое простое правило, которым, к сожалению, часто пренебрегают.

 1.3. Наличие на токене недекларированных возможностей («закладок») — получение несертифицированных ключевых носителей из ненадежных источников чревато наличием в программном обеспечении не заявленных в документации включений. Через эти «кротовые норы» преступники могут похитить закрытый ключ электронной подписи.

Нейтрализация: — приобретение сертифицированных ФСТЭК носителей — удостовериться в отсутствии «закладок» можно с помощью просвечивания usb-токена рентгеном, что осуществляется в лабораториях Федеральной службы технического и экспортного контроля. Если в результате исследования не было выявлено «закладок», то ключевой носитель признается безопасным и на него выпускают сертификат ФСТЭК.

 2) Технологичные преступления — для реализации подобных противоправных схем от мошенников в первую очередь требуются навыки в области IT-технологий и информационной безопасности.
 2.1. Внедрение злоумышленника в «машину» владельца электронной подписи — мошенник, получивший доступ к компьютеру или ноутбуку жертвы может похитить ключ, скопировав его, в случае если он извлекаемый, или использовать ЭП без ведома владельца. Соответственно, это позволит преступнику узнать пароль токена и получить доступ к электронной подписи, хранящейся на нем.

Нейтрализация: — выполнение правил информационной гигиены — не переходить по подозрительным ссылкам (обратите внимание, что в письме может быть написан адрес надежного сайта, но при наведении курсором может высветиться совершенно другой адрес гиперссылки), не скачивать программы и файлы из ненадежных источников, не пользоваться потенциально зараженными флешками, установить на компьютер или ноутбук антивирусную программу и прочее.

 2.2. Компрометация канала связи «токен-машина» — если злоумышленник проникает в канал передачи данных от usb-токена к компьютеру или ноутбуку, то это грозит, в зависимости от типа ключевого носителя, и компрометацией пароля, и компрометацией ключа.

 **Нейтрализация:** — выполнение правил информационной гигиены + ФКН — способ предотвратить реализацию подобной схемы, аналогичен предыдущему. В качестве дополнительного средства обезопасить электронную подпись от компрометации можно упомянуть функциональный ключевой носитель (ФКН). ФКН отличается тем, что разделяет вычисления во время генерации ЭП между пользовательским приложением и токеном таким образом, что данные, которые передаются по каналу связи, не позволят преступнику сделать никаких выводов ни о ключе, ни о пароле.

 3) Социальные преступления — мошеннические схемы, основанные на личных качествах людей, их способности имитировать других, вводить в заблуждение, подделывать документы. Подобные нарушения в большинстве своем сложно предупредить, но всем действующим и потенциальным владельцам ЭП нужно знать, что рынок нашел способ борьбы и с подобными преступлениями.

 3.1. Получение электронной подписи другим человеком — преступник может завладеть документами нужного лица (найти, украсть) и, используя максимально похожего на него соучастника, получить ЭП.

Нейтрализация: — ответственное отношение к документам — необходимо хранить документы в надежных местах, а в случае их кражи незамедлительно сообщать в правоохранительные органы.

 3.2. Получение электронной подписи по поддельным документам и доверенности — регламент рынка электронной подписи подразумевает обязательную личную явку при первичном получении ЭП, а при повторном выпуске забрать ее можно, предоставив копии необходимых документов и доверенность. Этим и могут воспользоваться мошенники, подделав бумаги.

 3.3. Недобросовестность сотрудников удостоверяющих центров — как и в любой системе, будь то правоохранительная, судебная или любая другая, ее рядовые пользователи зависят от тех, кто наделен полномочиями. Вот он наиболее негативный человеческий фактор — беззащитность перед находящимся «внутри» преступником. При подобных проникновениях любая система выходит из равновесия, и одна из самых надежных и легко приводимых в норму — это система выпуска электронной подписи.

 **Нейтрализация** схем 3.2. и 3.3.: — ответственное выполнение сотрудниками УЦ своих обязанностей — в этих случаях предотвращение возможно только внутри удостоверяющих центров при помощи слаженной работы менеджеров, выпускающих ЭП, служб информационной безопасности, подбора персонала и коллег потенциального злоумышленника, что и происходит на современном рынке ЭП. Но это по-прежнему не исключает человеческого фактора на 100%.

 Завладение чужой электронной подписью противоречит законодательству РФ и за него предусмотрена уголовная ответственность. «При этом данная категория дел отнесена к делам частно-публичного обвинения, что говорит о возбуждении уголовного дела и начале уголовного преследования только на основании заявления потерпевшего.
Одной из мер, направленных на защиту своего имущества, является подача заявления о невозможности государственной регистрации без личного участия правообладателя, подсказывают в Росреестре.