ПАМЯТКА ВЛАДЕЛЬЦУ **ЭЛЕКТРОННОЙ ПОДПИСИ**

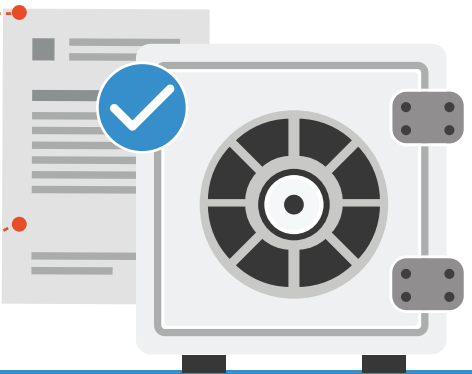
Риск | Способы минимизации негативных последствий

ЭТАП I. ПРИОБРЕТЕНИЕ ИЛИ ПОВТОРНЫЙ ВЫПУСК ЭЛЕКТРОННОЙ ПОДПИСИ

Получение "вашей" электронной подписи другим человеком по копиям документов или поддельным документам

Ответственное отношение к документам (защита от копирования случайными лицами)

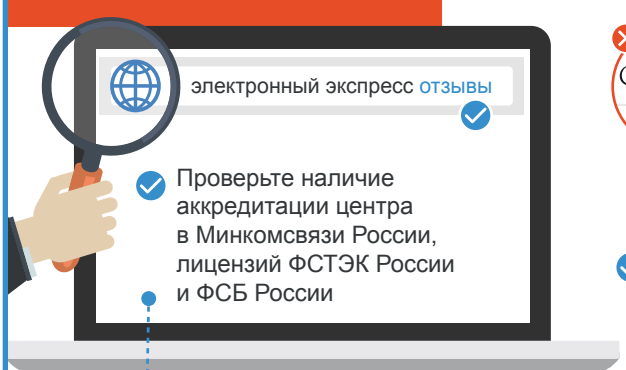
- Избегайте излишнего копирования документов при получении банковских или государственных услуг
- В случае кражи документов незамедлительно сообщите в правоохранительные органы и произведите их замену
- Избегайте отправки отсканированных копий документов по электронной почте даже в архиве с паролем



Ошибка при выборе удостоверяющего центра

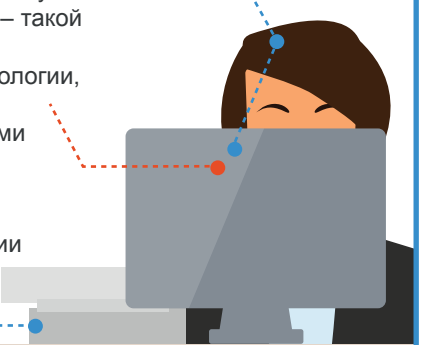
Ответственный подход к выбору удостоверяющего центра

- Помните, что незначительная экономия может привести к серьезным последствиям: так, для соблюдения требований идентификации личности, проверки документов и работы с персональными данными требуются квалифицированные сотрудники и хорошее программно-аппаратное обеспечение



- Проверьте наличие аккредитации центра в Минкомсвязи России, лицензий ФСТЭК России и ФСБ России

- Не соглашайтесь на дистанционный выпуск или продление электронной подписи – такой удостоверяющий центр работает по не предусмотренной законом технологии, а ваши данные при таком способе взаимодействия становятся уязвимыми



- Формирование ключа должно производиться самостоятельно клиентом или в его присутствии

- проверьте насколько давно работает выбранный центр, не приостанавливалась ли его аккредитация *(ссылка по QR-коду)*

- Внимательно прочитайте договор – стороной по договору должен быть удостоверяющий центр, аккредитованный Минкомсвязи России, а не посредник, не несущий никакой ответственности

Важно знать, что "старую подпись" нельзя "продлить". Технология в целях информационной безопасности предполагает каждый раз выпуск нового уникального ключа. Это значит, что все процедуры идентификации нужно пройти заново. И если вам предлагают "продлить старую подпись по облегченной процедуре", это повод насторожиться и выбрать более надежный удостоверяющий центр

Наличие на токене недекларированных возможностей ("закладок")

Приобретение только сертифицированных ФСТЭК России носителей

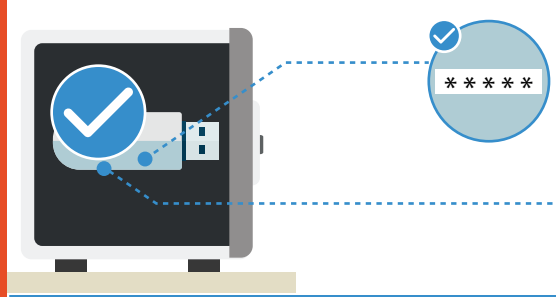
Использование ваших данных для оформления электронной подписи или для незаконных операций по доверенности с вашей недвижимостью в Росреестре

Необходимо подать заявление о невозможности регистрации перехода, прекращения, ограничения права и обременения объекта недвижимости без личного участия собственника в личном кабинете на сайте Росреестра или при личном обращении в МФЦ

ЭТАП II. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Физическая кража носителя

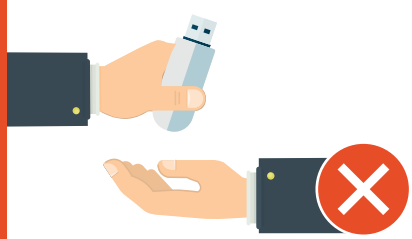
Соблюдение базовых правил информационной безопасности



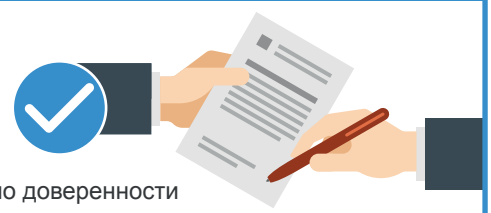
Немедленно аннулируйте сертификат ключа проверки электронной подписи при предположении, что носитель был украден, обратившись в удостоверяющий центр, который выдал сертификат ключа проверки электронной подписи с заявлением об отзыве сертификата

Добровольная передача своей электронной подписи другому лицу, например, директором бухгалтеру для подачи отчетности

Обеспечение режима использования электронной подписи только самим владельцем

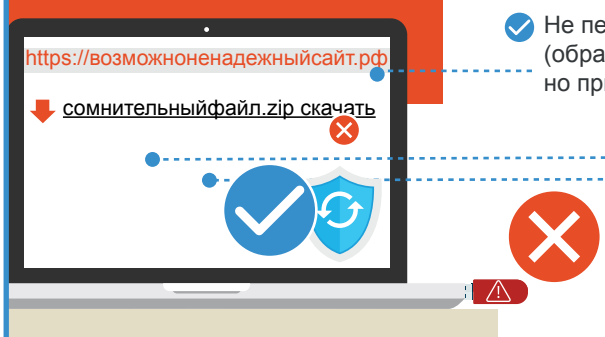


Выпустите электронную подпись для нужных сотрудников по доверенности



Шпионские программы, вирусы

Соблюдение правил информационной "гигиены"



Не переходите по подозрительным ссылкам, даже если указан адрес надежного сайта (обратите внимание, что в письме может быть написан адрес надежного сайта, но при наведении курсором может высветиться совершенно другой адрес гиперссылки)

ukrademdannye.ru

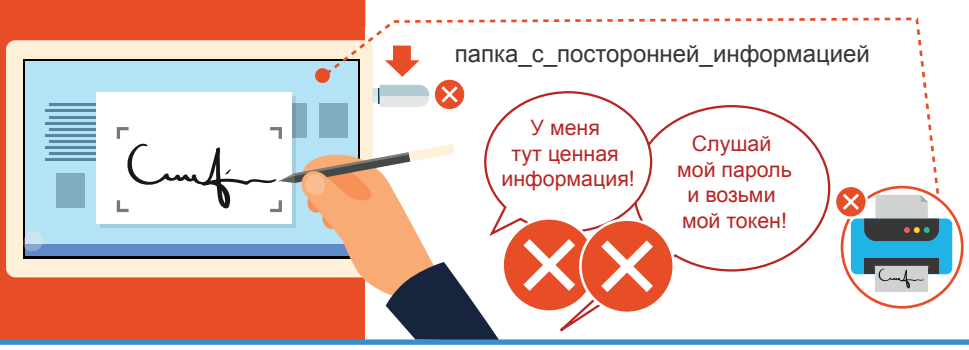
Поручайте администрирование программного обеспечения только доверенным лицам

Блокируйте компьютер на время временного отсутствия

ЭТАП III. ЗАВЕРШЕНИЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Компрометация электронной подписи

Предупреждение компрометации электронной подписи в ходе использования



Не вносите какие-либо изменения в программное обеспечение средства криптографической защиты информации

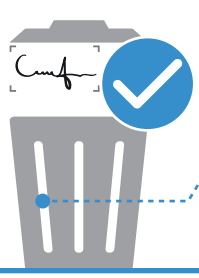
Немедленно аннулируйте сертификат ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи нарушена

К компрометации ключей можно отнести следующие события:

- утрата ключевого носителя (в том числе с последующим обнаружением)
- хищение
- передача ключевой информации по каналам связи в открытом виде
- несанкционированное копирование
- увольнение сотрудников, имевших доступ к ключевой информации
- любые другие виды разглашения ключевой информации

Перехват не используемых по различным причинам подписей

Предупреждение использования ключа без ведома владельца



Уничтожьте ключи электронной подписи в соответствии со сроками и порядком, установленными эксплуатационной документацией на средство криптографической защиты информации

Отзовите сертификат ключа электронной подписи при смене руководителя или сотрудника организации, обратившись в удостоверяющий центр с соответствующим заявлением