

За кражу электронной подписи могут дать до трёх лет тюрьмы

Посадят и самих мошенников, и сотрудников удостоверяющих центров, которые им помогли

Использование цифровой подписи, особенно за время пандемии, охватило многие сферы жизни: с её помощью можно удалённо заверить любые документы — от заявления в вуз до многомиллионных договоров. Однако правоохранители обнаружили, что даже самая надёжная цифровая подпись — усиленная квалифицированная — тоже может оказаться в руках мошенников. За преступления с её использованием МВД России предложило ввести уголовную ответственность, сообщил ТАСС 18 мая. «Парламентская газета» разобралась, какие риски могут ждать людей, решивших подписать что-либо дистанционно.

ПРЕСТУПНИКИ МОГУТ ВСЁ

Электронная подпись, по сути, то же самое, что и обычная подпись, но в цифровом виде. Она приравнивает любой документ в компьютере к бумажному оригиналу. С её помощью обычные люди, например, могут получить госуслуги через Интернет, подать заявление на поступление в вуз или записать ребёнка в садик, обмениваться документами с удалённым работодателем, а также отправить в суд иск или жалобу. Юристам и индивидуальным предпринимателям цифровая подпись открывает возможность дистанционно передавать налоговые декларации, регистрировать сделки с недвижимостью, оформлять банковские документы, участвовать в электронных торгах.

В зависимости от документа, который требуется заверить, нужны три вида подписи: простая, усиленная неквалифицированная и квалифицированная. Самой надёжной считается последняя: её выдают только в удостоверяющем центре, имеющем сертификацию ФСБ и аккредитацию Минцифры. Такая подпись и наиболее сложная: это USB-носитель, на котором записан ключ — специальный зашифрованный код. Работать с ним можно лишь после установки специальной программы.

Эксперты отмечают, что взломать такой код почти невозможно — это требует слишком больших вы-

числительных ресурсов. А если кто-то потеряет закрытый ключ, то по его сигналу удостоверяющий центр сразу отзывает сертификат и что-то подписать им становится нельзя.

Однако чем сложнее задача, тем больше мошенников, кажется, берёт азарт: они научились красть и подделывать даже этот вид подписи. В МВД рассказали, что злоумышленники получают ключи или сертификаты проверки элек-

184,9 тысячи

ИТ-преступлений произошло в России с начала года. Это на 31 процент выше по сравнению с аналогичным показателем прошлого года

тронной подписи, оформленные на другого человека, либо вводя в заблуждение сотрудника удостоверяющего центра, либо вступая с ним в сговор. Кроме того, преступники могут просто украсть флешку с ключом или купить ключ, оформленный на подставное лицо. Правоохранители зафиксировали, что в результате таких махинаций заметно увеличилось количество преступлений, связанных с открытием фирм с использованием



украденных подписей. Как отметил начальник Договорно-правового департамента МВД

России **Александр Авдейко**, с начала года количество ИТ-преступлений достигло 184,9 тысячи, что на 31 процент выше по сравнению с аналогичным показателем прошлого года, сообщили СМИ.

ДЕЛО РУК САМИХ УТОПАЮЩИХ

Если за подделку обычной подписи издавна существует уголовная ответственность, то за неправомерные действия с электронной

подписью предусмотрена лишь административная. Так, согласно статье 13.33 КоАП, если удостоверяющий центр выдал кому-либо сертификат электронной подписи, содержащий заведомо недостоверную информацию о его владельце, то его оштрафуют на 200–250 тысяч рублей. И на этом, в общем-то, всё. Учитывая степень опасности таких преступлений, МВД предложило ликвидировать пробел и ввести уголовное наказание как для похитителей ключа, так и для их подельников. Согласно разработанному ведомством законопроекту, за хищение цифровой подписи виновные заплатят штрафом от

На сколько могут посадить за подделку обычной подписи

На официальных документах — до двух лет

В паспорте или удостоверении — до трёх лет

За приобретение, хранение, сбыт поддельных паспортов, удостоверений или официальных документов — до одного года

100 до 300 тысяч рублей либо лишением свободы до трёх лет. А сотрудникам удостоверяющих центров, которые им способствовали, придётся выложить до 300 тысяч рублей или отправиться в колонию на три-четыре года.

Как подчеркнул «Парламентской газете» председатель общественной организации по защите прав потребителей «Общественная потребительская инициатива» **Олег Павлов**, такая инициатива совершенно справедлива, ведь сфера применения электронной подписи постоянно расширяется.

«Мы убеждены, что ответственность за её подделку должна быть максимально жёсткой, — сказал эксперт. — Люди применяют её как для создания компаний, так и для открытия счетов и направления обращений в органы власти. Для граждан растут риски в случае её неправомерного использования».

По его словам, сейчас, к сожалению, единственный способ обезопасить себя от кражи электронной подписи — это вообще не заводить её. «Однако удобства зачастую перевешивают риски, — признал Павлов. — Поэтому людям надо тщательно соблюдать так называемую цифровую гигиену, использовать решения с максимальной степенью защиты, двухфакторную аутентификацию и прочее».

АНАСТАСИЯ ЯЛАНСКАЯ
ФОТО PHOTOPRESS

Информационное сообщение АО «СО ЕЭС»

На официальном сайте АО «СО ЕЭС» (www.so-ups.ru) в разделе «Деятельность/Раскрытие информации субъектом рынка/Структура и объём затрат на производство и реализацию товаров (работ, услуг)» размещена информация о структуре и объёмах затрат на оказание услуг по оперативно-диспетчерскому управлению в электроэнергетике субъектами оперативно-диспетчерского управления (в части управления технологическими режимами и в части обеспечения системной надёжности) за 2020 год.

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ПУБЛИЧНОГО АКЦИОНЕРНОГО ОБЩЕСТВА «КВАДРА – ГЕНЕРИРУЮЩАЯ КОМПАНИЯ»

Размещается согласно Постановлению Правительства РФ от 21 января 2004 г. №24 «Об утверждении стандартов раскрытия информации субъектами оптового и розничных рынков электрической энергии».

Состав и характер раскрываемой информации:

Бухгалтерская отчётность на 31.12.2020 и аудиторское заключение.

Затраты на производство и реализацию товаров (работ и услуг) в 2020 году.

Информация о тарифах на поставку электроэнергии (решение и источник опубликования).

Информация о выбросах загрязняющих веществ, оказывающих влияние на окружающую среду в 2020 году, мероприятия по сокращению.

Информация об инвестиционных программах за 2020 год.

Расход электроэнергии на собственные и хозяйственные нужды генерирующего оборудования в 2020 году.

Информация об используемом топливе в 2020 году.

Информация в полном объёме размещена на сайте ПАО «Квадра» по адресу:

http://quadra.ru/shareholders/disclosure_of_information/market_actors/RaskrOREM_2020.pdf