Артем Магунов, старший юрист АБ «Егоров, Пугинский, Афанасьев и партнеры»
Андрей Тузов, старший юрист АБ «Егоров, Пугинский, Афанасьев и партнеры»

Электронная подпись
О новых рисках и угрозах

Электронный континуум все активнее проникает в нашу повседневную жизнь, принципиально изменяя привычную нам среду обитания. Мы уже не мыслим существование без того комфорта, который предоставляет виртуальное взаимодействие. Но любое преимущество, включая технологическое, влечет за собой не только новые блага, но и новые риски и угрозы. В настоящей статье речь пойдет об использовании электронной подписи при хищениях имущества и в иных преступлениях в сфере экономики. На примерах отчуждения недвижимости, регистрации юридического лица показан алгоритм действий злоумышленников, даны рекомендации для предотвращения подобных преступлений.

Злоумышленники идут в ногу с прогрессом, в связи с чем мы наблюдаем бурный рост противоправных действий с применением новых технологий.
Согласно данным МВД РФ:
– за период январь-декабрь 2017 г. зафиксировано 90 587 преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (раскрыто 20 424)[1];
– за январь-декабрь 2018 г. зарегистрировано 174 674 преступления, совершенные с использованием компьютерных и телекоммуникационных технологий (раскрыто 43 362)[2];
– а за пять месяцев 2019 г. уже совершено с использованием компьютерных и телекоммуникационных технологий 97 524 преступления (раскрыто 22 934), т.е. больше чем за весь 2017 г.[3]
Ранее злоумышленники, специализирующиеся на хищениях с помощью электронных технологий, в основном сосредотачивались на неправомерном доступе к персональным данным и списаниях денежных средств с банковских счетов. Для защиты от таких противоправных действий практика выработала более или менее работающие технические решения и алгоритмы поведения.
Но в конце 2018-го и начале 2019 г. появился совершенно новый тренд – использование электронной подписи при хищениях имущества и в иных преступлениях в сфере экономики.
В ряде СМИ и обсуждениях в интернете освещаются случаи, когда владельцы дорогостоящей недвижимости либо собственники прибыльного бизнеса узнают о том, что их собственность им больше не принадлежит, поскольку ранее был произведен переход прав на основании сделки, подписанной электронной подписью потерпевшего.

Как работает преступная схема
В большинстве случаев алгоритм действий злоумышленников следующий:
1. В удостоверяющем центре, расположенном, как правило, в городе, где потерпевший никогда не был, получается электронная подпись.

---

[1] https://media.mvd.ru/files/application/1241295

[2] https://media.mvd.ru/files/application/1518099

[3] https://media.mvd.ru/files/application/1595051

2. Далее с помощью электронной подписи совершается сделка по отчуждению имущества на лицо, которое даже не подозревает о своем участии в сделке («промежуточное звено»).
3. Через некоторое время с помощью незаконно полученной электронной подписи промежуточного звена имущество вновь продается. И так несколько раз.
Находящийся в конце цепочки «новый» недобросовестный собственник никак себя не проявляет продолжительное время, и потерпевший не догадывается об отчуждении своих активов.
При этом выявление цепочки перепродаж на ранних этапах – это чистое везенье. Так, в одном случае собственника квартиры заинтересовало, почему в квитанции на оплату жилищно-коммунальных услуг перестали указывать его фамилию.
В другом случае 100% владельцу общества, одновременно являющемуся генеральным директором общества с ограниченной ответственностью, из налоговой поступил звонок о расхождениях в данных отчетности, поданной по каналам электронной связи.
И в том, и другом случае потерпевшие смогли пресечь реализацию преступной схемы по дальнейшему отчуждению их имущества.
Возникает закономерный вопрос: как получилось, что подобные преступления стали возможными и как предотвратить их в дальнейшем?

Отчуждение квартиры
Чтобы разобраться в проблеме, предлагаем рассмотреть ее на простом примере отчуждения квартиры. Для этого проанализируем процедуру перехода права на недвижимое имущество, совершенного на основании сделки, подписанной электронной подписью.
Согласно ст. 18 Федерального закона от 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости» заявление о государственной регистрации прав и прилагаемые к нему документы представляются в Росреестр в том числе в форме электронных документов и (или) электронных образов документов, подписанных усиленной квалифицированной электронной подписью, с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети «Интернет», посредством единого портала государственных и муниципальных услуг или официального сайта, или иных информационных технологий взаимодействия.
В случае представления заявления о государственной регистрации прав и прилагаемых к нему документов посредством отправления в электронной форме такие заявление и документы представляются путем заполнения формы заявления, размещенной на едином портале государственных и муниципальных услуг, официальном сайте Росреестра, с прикреплением соответствующих документов.
Согласно «Административному регламенту Федеральной службы государственной регистрации, кадастра и картографии по предоставлению государственной услуги по государственному кадастровому учету и (или) государственной регистрации прав на недвижимое имущество», утвержденному приказом Минэкономразвития России от 7 июня 2017 г. № 278, документы, необходимые для осуществления государственной регистрации прав и представляемые в форме электронных документов, должны подписываться усиленной квалифицированной электронной подписью уполномоченных на то лиц, сторон договора.
Сформированный комплект документов должен быть подписан усиленной квалифицированной электронной подписью заявителя.
При положительном рассмотрении заявления Россреестром вносится соответствующая регистрационная запись. При этом специальная регистрационная надпись на документе, выражающем содержание сделки и представленном в форме электронного документа, подписывается усиленной квалифицированной электронной подписью государственного регистратора.

Далее сотрудник Росреестра, ответственный за выдачу (направление) документов, осуществляет выдачу (направление) документов, подготовленных по результатам рассмотрения заявления, и необходимых документов в форме электронных документов с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети «Интернет», включая единый портал, посредством направления ссылки на электронный документ, размещенный на официальном сайте, по указанному в заявлении адресу электронной почты или направления электронного документа с использованием веб-сервисов.

Казалось бы, данный порядок в принципе исключает возможность отчуждения имущества без ведома его собственника, а также иных злоупотреблений при совершении сделки.

Как мы видим, на всех ключевых этапах присутствует усиленная квалифицированная электронная подпись. При этом существует мнение, что для подделки электронной подписи потребуется более 250 лет работы компьютера мощностью 100 млрд операций в секунду[4]. Очевидно, что при таких условиях подделка электронной подписи злоумышленниками маловероятна.

Слабое звено

Однако слабым звеном в данном случае является все же электронная подпись (точнее этап получения сертификата ключа проверки электронной подписи и дальнейшее хранение электронной подписи) и вот почему.

В настоящее время отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных законами, регулируются Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Закон об ЭП).

Согласно ст. 2 указанного закона 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.

Статья 5 Закона об ЭП различает два вида электронной подписи:

1) простая электронная подпись и

2) усиленная электронная подпись, представленная:

– неквалифицированной электронной подписью, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи;

– квалифицированной электронной подписью, которая обладает всеми признаками неквалифицированной электронной подписи и следующим дополнительным признаком: ключ проверки указан в квалифицированном сертификате, а для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Законом об ЭП.

При этом ст. 2 Закона об ЭП установлено, что сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

---

[4] *Петраков А.В., Лагутин В.С.* Защита абонентского телетрафика. М., 2001.

Квалифицированный сертификат ключа – сертификат ключа проверки электронной подписи, соответствующий установленным законодательством требованиям и созданный аккредитованным удостоверяющим центром либо уполномоченным федеральным органом.

При этом удостоверяющим центром является юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей.

На территории Российской Федерации Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации аккредитованы более 400 удостоверяющих центров[5].

Какого-либо общего реестра выданных электронных подписей на настоящий момент не существует.

Таким образом, в современных условиях нельзя исключать вероятность получения электронной подписи в удостоверяющем центре не самим гражданином, а иным лицом, в том числе без его ведома, например, с помощью методов социальной инженерии. В частности, как указывалось выше, злоумышленники предпочитают получать электронную подпись в местах, максимально удаленных от места жительства гражданина[6].

Реализовав свой умысел, злоумышленник получает инструмент, позволяющий не только распоряжаться имуществом законопослушного гражданина, но также совершать от его имени иные действия в рамках противоправной деятельности, например, направлять в регистрирующий орган сведения о регистрации ИП, юридического лица, вносить искаженные сведения в отчетность. В последнем случае получение электронных подписей злоумышленниками причиняет вред не только физическим лицам, но и бизнесу.

В частности, известна схема, когда после корректировки деклараций и отчетов у злоумышленников при определенных условиях появляется хоть и сложно реализуемая, но возможность получать возвраты по переплатам.

Еще одним случаем, порождающим возможность преступного использования электронной подписи, является банальное несоблюдение лицом условий хранения носителя (токена) с цифровой подписью, владельцем сертификата ключа которой он является. Передача токена третьим лицам, бесконтрольное нахождение носителя в общедоступном месте, несвоевременное получение в удостоверяющем центре – все это также может привести к вышеуказанным последствиям.

По нашему мнению, двумя ключевыми предпосылками существования вышеуказанных рисков является то, что, с одной стороны, у нас низкий уровень культуры обращения с персональными данными, а, с другой, отсутствует какой-либо единый реестр выданных электронных подписей, который позволял бы самому человеку отслеживать сведения о полученных на его имя электронных подписях, чтобы своевременно реагировать на появление несанкционированно выданных экземпляров, блокируя их по заявлению.

Но что делать, если злоумышленники все же реализовали преступный умысел и похитили имущество с использованием электронной подписи?

Действия потерпевшего

Конечно, с точки зрения гражданско-правовых последствий та же сделка отчуждения квартиры, совершенная от имени лица с помощью незаконной полученной электронной

---

[5] https://digital.gov.ru/ru/activity/govservices/2/

[6] Принятый в августе 2019 г. Закон № 286-ФЗ «О внесении изменений в Федеральный закон “О государственной регистрации недвижимости”» формально исключил возможность злоумышленникам использовать вышеописанный способ присвоения недвижимого имущества. Теперь отчуждение на основании документов, подписанных электронной подписью, будет возможно только при условии, если собственник прямо завил об этом в Россреестр, а последний указал об этом в ЕГРН. Между тем иные риски данный Закон не нивелирует.

подписи, является ничтожной ввиду отсутствия воли правообладателя. В этом случае ситуация аналогична использованию преступниками рукописной поддельной подписи.

Между тем необходимо учитывать, что согласно ч. 1 ст. 65 АПК РФ и ч. 1 ст. 56 ГПК РФ каждая сторона должна доказать те обстоятельства, на которые она ссылается как на основания своих требований и возражений.

При этом формально в вышеуказанных обстоятельствах электронная подпись не является поддельной и доказать ее неправомерное использование будет очень непросто. Сбор доказательной базы в подобном деле представляется весьма затруднительным. Исходя из нашей практики, можем утверждать, что объяснение заявителя о том, что он не обязан доказывать отрицательный факт, вряд ли удовлетворит суд.

Потребуется не только представить подтверждения того, что истец не получал и не мог получить электронную подпись, но убедительно объяснить причину, по которой он не знал о факте выдачи и (или) использовании электронной подписи.

В такой ситуации полагаем, что оптимальным решением будет ведение двух параллельных процессов: гражданско-правового спора и инициирование уголовного расследования.

Полученные в рамках уголовного расследования доказательства (в том числе допросы, результаты обысков и выемок), по нашему мнению, могут существенно усилить позицию в гражданско-правовом споре.

При этом в уголовной части кейса необходимо учитывать следующее. В уголовно-правовом смысле электронная подпись сама по себе на сегодняшний день не попадает под самостоятельный объект уголовно-правовой охраны. Уголовный кодекс не предусматривает возможности привлечь к ответственности сотрудников удостоверяющих центров, выдавших в нарушение действующих правил электронную подпись третьему лицу. При этом не предусмотрена самостоятельная уголовная ответственность ни за действия, совершенные умышленно (когда они знали и понимали, что выдают в нарушение правил), ни по неосторожности (когда сотрудник должен был проявить внимательность при проверке предоставленных документов, но не проявил ее). Сам злоумышленник, получив электронную подпись за другого гражданина и не использовав ее в противоправных целях, тоже не может быть привлечен к уголовной ответственности[7].

Таким образом, электронная подпись в уголовно-правовом значении может выступать лишь орудием преступления, а применение электронной подписи – способом совершения преступления. Ярким примером тому служит приведенный случай с отчуждением (дарением) дорогостоящей квартиры. Понятно, что правоприменителю ничего не остается, как квалифицировать любую попытку отчуждения имущества владельца с применением электронной подписи, полученной злоумышленником, лишь как мошенничество, поскольку регистрирующий орган был введен в заблуждение относительно действительности выражения воли реального собственника при заключении соответствующей сделки.

Следовательно, в рамках расследования таких хищений в соответствии со ст. 73 УПК РФ адвокатам необходимо следить за установлением дополнительных обстоятельств совершения преступления и ходатайствовать о корректировке отклонений. К таким обстоятельствам относятся следующие:

1. В каком удостоверяющем центре была выдана использованная электронная подпись? Имеет ли этот удостоверяющий центр все необходимые документы для осуществления деятельности по выдаче электронных подписей (уставные документы, лицензии и сертификаты)?

---

[7] Во всевозможных концептуальных документах органов власти относительно роли и значения распространения электронной подписи последняя позиционируется в качестве альтернативы личному обращению в органы государственной власти с предъявлением паспорта гражданина, а вот за использование, изготовление или даже хранение поддельного паспорта меры правовой ответственности установлены.

2. При предъявлении каких документов была инициирована процедура изготовления и выдачи электронной подписи?
3. Кто именно обратился в удостоверяющий центр? Где взял документы, предъявив их сотруднику центра для получения подписи?
4. Имелся ли сговор между злоумышленником и сотрудником удостоверяющего центра?
5. Не была ли нарушена процедура выдачи электронной подписи удостоверяющим центром?

Естественно, в данном контексте должны быть произведены соответствующие выемки документов – оснований выдачи электронной подписи, допросы сотрудников удостоверяющего центра относительно обстоятельств обращения злоумышленника, отработаны в оперативно-розыскном порядке связи и контакты, чтобы исключить наличие сговора. Соответственно, если адвокат сталкивается с представлением интересов потерпевшего в такого рода делах, необходимо принимать меры к тому, чтобы комплекс этих обстоятельств был установлен следствием. Это будет полезно и с точки зрения будущей защиты материальных интересов потерпевшего, ведь следственные органы могут собрать доказательства, которые можно будет использовать в обосновании исковых требований, направленных на возмещение причиненного ущерба. Вполне возможно, что из материалов уголовного дела будет просматриваться вина удостоверяющего центра, соответственно, это повысит шансы получить реальное возмещение ущерба.

Регистрация юридического лица

В своей практике мы также отмечаем рост числа случаев использования электронной подписи и при совершении ряда других противоправных действий, например, регистрации юридических лиц. На гражданина, чьи персональные данные смогли раздобыть, получается электронная подпись, с применением которой подаются документы на регистрацию обществ с ограниченной ответственностью, где этот гражданин выступает генеральным директором или единственным участником. Конечно же, сам гражданин, на кого таким образом было зарегистрировано юридическое лицо, узнает об этом либо случайно (например, при прохождении проверки служб безопасности при получении кредитов, звонков из банков), либо когда правоохранительными органами расследуется преступление и этого человека вызывают на опрос или допрос в связи с уклонением от уплаты налогов или совершением каких-либо мошеннических действий.

В этой ситуации логика работы следственных органов по установлению обстоятельств совершения преступления будет меняться. В частности, речь идет о доказывании ч. 1 ст. 170.1 УК РФ (фальсификация единого государственного реестра юридических лиц), в рамках которой следственные органы должны истребовать из регистрирующего органа документы, заявление и другие материалы, предоставленные злоумышленником, после чего необходимо установить удостоверяющий центр и обстоятельства получения электронной подписи по аналогии с вышеуказанными действиями. Важно проработать связи злоумышленников, проверить их действия на согласованность и единый умысел, чтобы исключить признаки других преступлений.

Несмотря на то что правоприменительная практика по ч. 1 ст. 170.1 УК РФ не такая большая, за расследование данного уголовного дела придется болеть, поскольку его исход и результаты во многом будут упрощать процесс доказывания в арбитражном суде по признанию соответствующей записи в ЕГРЮЛ недействительной, что может иметь огромное репутационное значение для бизнеса, например, если в результате такой несанкционированной смены генеральный директор был из региона, с которым может быть связан риск применения санкций иностранными государствами – контрагентами предприятия.

В любом случае будет полезным получить из материалов уголовного дела допросы сотрудников удостоверяющего центра, изъятые документы – основания выдачи электронной подписи, особенно если речь идет о предъявлении злоумышленниками в

удостоверяющий центр подложного паспорта гражданина (например, с измененной фотографией и т.д.).
Полезным будет также и получить протокол, в котором будет отражено, что носитель сомнительной электронной подписи был изъят у злоумышленника.
Таким образом, если электронную подпись человек не получал, то вполне можно рекомендовать регулярно проверять ЕГРЮЛ на наличие оформленных на себя фирм (делать это удобно через сервисы в сети «Интернет»).
В случае обнаружения фирмы, в которой человек указан в роли генерального директора или участника, но фактического отношения к ней не имеет, в кратчайшие сроки подать в регистрирующий орган (ИФНС) форму Р38001[8].
В связи с вступлением 13 августа 2019 г. в силу Федерального закона от 2 августа 2019 г. № 286-ФЗ, которым внесены поправки в Федеральный закон от 13 июля 2015 г. № 218-ФЗ «О государственной регистрации недвижимости», перед регистрацией сделок с недвижимостью с применением усиленной квалифицированной электронной подписи необходимо подать личное заявление в Росреестр. Поэтому достаточно лишь запросить актуальные выписки из Единого государственного реестра недвижимости с целью проверки, все ли объекты недвижимости принадлежат вам.
С другой стороны, если речь идет о преступлении, которое было совершено с использованием незаконно полученной подписи, а ее владелец ранее использовал эту электронную подпись, с помощью которой было совершено хищение или другое преступление, в этом случае необходимо будет представить убедительные доказательства того, что эта электронная подпись действительно не использовалась потерпевшим и выбыла из его обладания на момент совершения преступных действий.
Электронная подпись, будучи аппаратно-программным или только программным продуктом, уязвима как от физической утраты (хищения) носителя, так и от утечки данных с компьютера пользователя в связи с использованием нелицензионного программного обеспечения либо наличия на нем вредоносных программ. В средствах массовой информации встречается много примеров того, как у пользователей, не заметивших пагубного влияния вирусов, перечислялись денежные средства с расчетных счетов по подставным реквизитам в дистанционных системах банковского обслуживания. При этом использованная электронная подпись была оригинальной.

***

Из рассмотренных примеров можно выделить две рекомендации для защиты:
1) обеспечить максимально безопасное хранение токена, никогда не терять, не передавать третьим лицам носитель электронной подписи ни под каким предлогом;
2) соблюдать должные меры информационной защиты и безопасности каналов связи и используемой в работе техники.

[8] Возможно также подать форму Р38001, в которой можно отразить свое неучастие в множестве юридических лиц, или в целом. Однако такое заявление должно подаваться в каждый регистрирующий орган лично, и в связи с этим мы не считаем это высокоэффективным средством защиты от потенциальной угрозы регистрации юридического лица без ведома гражданина.