УДК 340

Бондаренко Юрий Алексеевич
кандидат юридических наук,
доцент кафедры криминалистики и правовой информатики,
Кубанский государственный университет
Bondarenko_yuri@mail.ru
Yuri A. Bondarenko
PhD in Law,
associate Professor of the forensic science and
legal informatics department at Kuban State University
Bondarenko_yuri@mail.ru

Особенности расследования мошенничества, совершенного с использованием электронной подписи

Some features of the fraud investigation which doing by means of a digital signature

Аннотация. *В статье рассматриваются различные способы совершения мошенничества с использованием злоумышленниками средств электронной подписи. Выявлены закономерности использования технологии электронной подписи при выборе способа совершения и сокрытия следов преступления. Также, автором приводятся примеры типичных следов, образующихся после его совершения и правила их поиска, изъятия и фиксации. Автор выявлены некоторые обстоятельства, подлежащие установлению при расследовании мошенничества этого вида.*

Ключевые слова: *электронная подпись, хеш-функция, мошенничество, обман, расследование, следы преступления, место происшествия.*

Summary *The article reviews some ways of a fraud by means of a digital signature. The mechanism of using this tool was detected during of its execution and concealment. Also it puts into the typical traces and the rules of their searching, withdrawing and fixation. The author submits some circumstances with the fraud investigation.*

Keywords: *a digital signature, the hash function, a fraud, a deceive, an investigation, traces of a crime, a crime scene.*

Информационные технологии активно проникают в повседневную деятельность органов государственной власти и местного самоуправления, организаций и граждан. Оптимизируя процедуры управления, учета, расчетов, диагностики и прогнозирования в социальных системах, они кардинально изменили бытие личности, общества и государства в планетарном масштабе [1, с. 10-13]. Поэтому не вызывает никаких сомнений утверждение о выявленной глобальной корреляции количества мошенничеств с использованием различных электронных средств коммуникации [2, с. 588].

Сегодня информационные технологии и носители информации являются неотъемлемой частью производительных сил общества, в том числе, в сфере правоприменения. Здесь необходимо отметить такие направления, как электронный документооборот, электронная подпись, гражданско-правовой институт цифровых прав, а также находящиеся на рассмотрении Федерального Собрания Российской Федерации законопроекты о цифровых финансовых активах и об альтернативных способах привлечения инвестиций (краудфандинге).

Конечно, новые технологии не остались незамеченными и преступным сообществом. В частности, анализ судебно-следственной практики позволяет нам говорить о попытках внедрения в процесс совершения преступлений технологии электронной подписи для удостоверения с ее помощью сделок от имени третьих лиц по отчуждению и (или) принятию имущества без их согласия и надлежащего уведомления, как того требует законодательство.

Использование электронной подписи преступниками позволяет им:

- лишать собственника принадлежащего ему имущества;
- получать денежные средства от имени других лиц в кредитных и микрофинансовых организациях;
- незаконным путем производить смену собственника юридического лица;
- лишать участника гражданско-правовых правоотношений возможности подачи заявок на конкурсные процедуры в сфере закупок для государственных и муниципальных нужд при хищении подписи.

Осуществляя анализ способов совершения мошенничеств с использованием электронной подписи, стоит указать на две группы таких способов: технические (технологические) и социального взаимодействия.

Среди способов технического характера выделим создание на физическом носителе из ненадежного источника электронной подписи программы-шпиона, которая может получить доступ к коду подписи и коду ее проверки. Другим средством противоправного получения сведений о ключе подписи и ее проверки является внедрение в компьютер пользователя подписи вредоносных программ с последующем получением данных о ключе подписи и ключе проверки.

Способы мошенничества на основе социального взаимодействия более распространены и разнообразны, начиная от тайного хищения носителя подписи до введения в заблуждение сотрудников удостоверяющего центра или их незаконные действия по выдаче электронной подписи неуполномоченному лицу. Здесь можно указать и на получение подписи по поддельным документам, в том числе, заверенным нотариусом доверенностям.

Так, получила широкую огласку ситуация, когда собственник недвижимости был лишен своего права путем совершения фиктивного договора купли-продажи, заверенного его электронной подписью. Было установлено, что потерпевший никогда не оформлял электронную подпись в удостоверяющих центрах и органах государственной власти. Однако

злоумышленники воспользовались его скан-копией паспорта гражданина Российской Федерации, добыли информацию из электронной системы оказания государственных услуг и подделали личную подпись для выдачи электронной подписи. Удостоверяющий центр не произвел надлежащим образом сверку представленных документов и выдал на имя гражданина электронную подпись, которая, в свою очередь, использовалась для удостоверения сделки по отчуждению недвижимого имущества в пользу третьего лица без согласия собственника.

Приступая к рассмотрению особенностей выявления и расследования мошенничеств этого вида, следует отметить, что они совершаются профессиональными организованными преступными группами, использующими уязвимости технологии электронной подписи программно-технического и юридического характера в противоправных целях. Специфика способов мошенничества предопределена порядком формирования и выдачи подписи аккредитованным центром, положениями гражданского законодательства о ее использовании, алгоритмом проверки подписи. На всех этапах работы с электронной подписью происходит формирование специфических следов, в том числе и электронной природы.

Технической и программной предпосылкой формирования усиленной квалифицированной электронной подписи выступает технология хеширования. Она представляет собой метод асимметричного шифрования с последующим сравнением двух сформированных кодов получателем информации и аутентификации отправителя (подписанта).

Современная следственная практика показывает, что на стадиях подготовки и совершения преступления используются закономерности генерирования электронной подписи и каналов проверки ее подлинности. Преступники изучили технологию хеш-проверки электронной подписи и нашли в ней некоторые уязвимости. Главной из них выступает «человеческий фактор», причиной которому – несовершенство законодательного регулирования отношений между уполномоченным центром, заказчиком подписи и пользователем, субъектами проверки подлинности подписи. Еще одна уязвимость электронной подписи – это возможность подделки сертификата проверки ключа электронной подписи. Здесь необходимо отметить, что такой сертификат выдается для возможности проверки подлинности подписи третьими лицами при использовании электронной подписи. Технология хеш-проверки проявляется в изначальном формировании двух разных электронных кодов, один из которых выступает собственно содержанием электронной подписи, а другой связывает электронную подпись с удостоверяющим центром, выдавшим ее на имя владельца.

Не затрагивая здесь самой технологии криптографического обеспечения электронной подписи, отметим, что в Российской Федерации сегодня применяются два различных стандарта проверки квалифицированных сертификатов проверки ключей электронных подписей. Используются схемы электронной подписи по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, получаемые

файлы подписей обычно имеют формат «.sig», «.sgn», «.p7b» для подписания электронных документов в Росреестре и последующей государственной регистрации перехода права на недвижимое имущество. Поэтому сам процесс создания и аутентификации пользователя усиленной квалифицированной электронной подписи практически невозможно сфальсифицировать без параллельного подбора алгоритма генерирования ключей проверки подписи специализированным программным обеспечением [3].

Сертификат ключа проверки электронной подписи включает в себя разнородную информацию о сроках действия такого сертификата и его номере в реестре:

- данные о владельце сертификата, его идентификационных номерах налогоплательщика и системы социального страхования;
- уникальный ключ проверки подписи;
- указание на используемое средство при создании подписи и средств аккредитованного удостоверяющего центра;
- название и место нахождения удостоверяющего центра, ограничения по использованию сертификата.

Однако экономика и логика организованной преступной деятельности на современном этапе мотивирует ее представителей к совершению мошенничеств с использованием средств электронной подписи только в случае высокой стоимости имущества, на которое направлено посягательство, а также - возможность его скорой реализации. Практика показывает, что в Российской Федерации не зарегистрированы мошенничества, совершенные способом подбора ключей электронной подписи с созданием ее дубликата. Это подтверждает высокую надежность применяемой технологии криптографической защиты информации.

В настоящее время мошенничество с использованием электронной подписи совершается путем нарушения установленного законом порядка ее выдачи и использования субъектами взаимодействия [4].

Л.А. Латыпова обоснованно указывает на ненадежность носителей электронной подписи на смарт-картах, что позволяет преступным группам завладевать хранящейся на ней информацией. В частности, «ключ подписи может быть с микропроцессорной карты; ключи электронной подписи часто производятся в так называемых удостоверяющих центрах, а затем загружаются на смарт-карту. Во многом это вопрос доверия к удостоверяющему центру, имеющего возможность сохранить копию этого ключа» [5, с.124-125].

Гражданин, индивидуальный предприниматель или единоличный исполнительный орган юридического лица получают усиленную квалифицированную электронную подпись при обращении в удостоверяющий центр и заключении с ним договора о предоставлении подписи, в том числе и в органах государственной власти. Получение преступниками информации о ключе подписи, ее копирование происходит либо в результате похищения смарт-карты с последующим возвратом для обнаружения владельцем, либо от сотрудника удостоверяющего центра.

Стоит сказать, что сотрудник удостоверяющего центра, обладая персональными данными гражданина, достаточными для выдачи электронной подписи, включая заявление и доверенность на ее получение третьим лицом, наделен правом по ее созданию и выдаче сертификата проверки ключа. Сама же технология создания и проверки ключа электронной подписи с использованием криптографических средств защиты обеспечивает достаточную надежность шифрования и проверки при использовании участниками электронного взаимодействия.

Приготовление, совершение и сокрытие мошенничеств с использованием средств электронной подписи закономерно влечет образование следов воздействия преступника на окружающую обстановку. Здесь необходимо разделять следы материальные, идеальные и электронные. При этом работа с электронными следами требует привлечения специалистов, обладающих специальными знаниями в области информационных технологий, компьютерной техники и диагностики компьютерных систем.

Специфику расследования такого вида преступлений составляет установление и процессуальное закрепление следов совершенного преступления, а они остаются в силу закономерностей правового и технического режима использования подписи. Типичными следами по делам этого вида выступают:

- устройства-электронные накопители информации с файлами, имеющими формат электронной подписи;
- сертификаты ключей проверки электронной подписи на электронном и (или) бумажном носителях;
- договоры и бухгалтерские документы с удостоверяющим центром о создании и выдаче электронной подписи;
- компьютерные файлы в виде электронных документов, подписанные электронной подписью;
- программное обеспечение для проверки подлинности сертификатов ключей электронной подписи, а также смартфоны с хранящейся в них информацией.

По своей природе, изымаемые следы преступной деятельности являются электронными. Пожалуй, одно из лучших определений электронных следов предложил А.А. Бессонов, согласно которому это «информация, зафиксированная в цифровом формате, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, причинно связанная с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника» [6, с. 47].

Выявление следов преступления часто происходит во время проведения осмотра места происшествия и предъявляемых заявителями предметов и документов при подаче заявления о преступлении. Еще один путь установления следов мошенничества с применением электронной подписи – производство

выемок и обысков в удостоверяющем центре, в местах хранения документов его руководителей или назначенных ими лиц. Однако для достижения внезапности следственно-оперативная группа нередко производит осмотр места происшествия в помещениях удостоверяющего центра. Осмотру подвергаются не только документы и компьютерная техника сотрудников центра, но и содержание электронных файлов специалистов и руководителей, проводивших операции по созданию и передаче ключа электронной подписи и сертификата ее проверки.

А.И. Анапольская рекомендует следователям при осмотре электронного документа зафиксировать наименование файла, его нахождение в корневом каталоге и путь к нему, а также формат файла. После этого следует указать в протоколе название файла, справочную характеристику о нем, затем выявить информацию, содержащуюся в самом документе и связанные с данным электронным документом другие электронные документы, сведения из которых имеют доказательственное значение [7, с. 17].

Обстоятельствами, подлежащими установлению при расследовании мошенничеств этого вида, которые детализируют предмет доказывания, выступают:

− наличие законного режима обладания имуществом потерпевшим до совершения преступления;

− выдача уполномоченным центром электронной подписи на имя потерпевшего при отсутствии его надлежащего уведомления;

− использование персональных данных потерпевшего для совершения подлога при выдаче электронной подписи на его имя;

− факт использования электронной подписи при заключении договора по отчуждению имущества, принадлежащего потерпевшему;

− переход права собственности от потерпевшего к другому лицу для реализации имущества или совершения других незаконных сделок с ним.

Обман как необходимое условие мошенничества имеет в исследуемом случае сложную многокомпонентную структуру. Его целью является маскировка незаконных действий преступников под видом гражданско-правовых отношений для недопущения их разоблачения.

Подводя итог, отметим, что новые принципы шифрования и проверки, хотя и обладают высокой степенью надежности кодирования информации, не защищают пользователей от недобросовестных действий со стороны сотрудников удостоверяющего центра и связанных с ними лиц. Законодатель предпринял меры по нейтрализации последствий несанкционированного использования электронной подписи обязанностью личного присутствия продавца при сдаче пакета документов для государственной регистрации перехода права собственности на недвижимое имущество.

Литература:

1. Дзидзоев Р.М. Институты электронной (цифровой) демократии в России // Юридический вестник Кубанского государственного университета. 2019,№ 2.

2. Садаф Р. Исследование влияния глобальной сети на финансовое мошенничество: международный обзор / Р. Садаф; Д. Олах; Д. Попп; Д. Мате // Устойчивое развитие, 2018. Т. 1. (англ.)

3. Робби Р. Предотвращение противоречия данных с помощью метода переполнения хэширования в закрытом процессе поиска хэша / Рахим Робби; Нурджамия и Ари Рафика Дьюи // Журнал физики: серия конференций. 2017, Vol. 930, Конференция 1. (англ.)

4. О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг: постановление Правительства Российской Федерации от 25.06.2012 г. № 634 (в ред. от 27.08.2018 г.) // Справочная правовая система «Консультант Плюс»

5. Латыпова Л.А. Методы защиты от фальсификации электронной подписи / Л.А. Латыпова; Л.А. Бахимова; Л.Х. Мифтахова // Вестник Казанского технологического университета. 2016. Т. 19. № 14.

6. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета им. О.Е. Кутафина. 2019, № 3.

7. Анапольская А.И. Особенности тактики проведения обыска по делам о мошенничествах, совершаемых в сфере проведения электронных расчетных операций // Вестник экономической безопасности. 2016, № 2.

References:

1. Dzidzoev R. M. Institutes of electronic (digital) democracy in Russia // Legal Bulletin of the Kuban state University. 2019, No. 2.

2. Sadaf R. An Investigation of the Influence of the Worldwide Governance and Competitiveness on Accounting Fraud Cases: A Cross-Country Perspective / Rabeea Sadaf; Judit Oláh; Józcef Popp; Domicián Máté // Sustainability, 2018. Vol. 10.

3. Robbi R. Data Collision Prevention with Overflow Hashing Technique in Closed Hash Searching Process / Rahim Robbi; Nurjamiyah and Arie Rafika Dewi // Journal of Physics: Conference Series. 2017, Vol. 930, Conference 1.

4. About types of electronic signature, the use of which is allowed when applying for state and municipal services: decree of the Government of the Russian Federation of 25.06.2012 No. 634 (as amended from 27.08.2018) // Reference legal system "Consultant Plus"

5. Latypova L.A. Methods of protection against falsification of electronic signatures / L.A. Latypova; L.A. Khakimova; L.H. Miftakhova // Bulletin of the Kazan technological University. 2016. Vol. 19. No. 14.

6. Bessonov A. A. About some possibilities of modern criminalistics in working with electronic traces // Vestnik Universiteta after O.E. Kutafin. 2019, No. 3.

7. Anapolskaya A.I. Features of search tactics in cases of fraud committed in the field of electronic settlement operations // Bulletin of economic security. 2016, No. 2.