УДК 343;31

Д. Б. ДУБОВИЧ
Луганський інститут МАУП

СПОСОБИ ПІДРОБЛЕННЯ ДОКУМЕНТІВ У СТРУКТУРІ МЕХАНІЗМУ ЗЛОЧИННИХ ТЕХНОЛОГІЙ ЗБАГАЧЕННЯ

Наукові праці МАУП, 2010, вип. 4(27), с. 119–123

При скоєнні економічних злочинів, які є основою злочинних технологій збагачення, документи стають предметами посягання з метою їх подальшого використання як засіб підготовки та скоєння злочину, а властивості підробленого документа мають вплив на умови та характер їх використання. Доведення підробки документів має свої відмінності і специфіку, яку потрібно враховувати при розслідуванні як основних злочинів, так і підробки документів та їх використання.

Досліджувана проблема ґрунтується на основних положеннях Конституції України, Кримінального Кодексу України та інших нормативних актах.

Розглянемо способи підроблення документів у структурі механізму злочинних технологій збагачення.

Як свідчить аналіз слідчої практики і спеціальної літератури, документи, що складаються і використовуються у господарюванні, підроблюються та використовуються у вигляді засобів скоєння таких економічних злочинів, як заволодіння чужим майном (ст. 190, 191 КК), фіктивне підприємництво (ст. 205 КК), ухилення від сплати податків (ст. 212 КК), шахрайство з фінансовими ресурсами (ст. 222 КК), легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом (ст. 209 КК) та ін. [1]. При скоєнні зазначених злочинів, які є основою злочинних технологій збагачення, документи стають предметами посягання з метою їх подальшого використання як засіб підготовки та скоєння злочину, а властивості підробленого документа мають вплив на умови та характер їх використання. В механізмі злочинних технологій збагачення неправдиві документи виступають єдиним або найбільш поширеним засобом досягнення злочинної мети — незаконного заволодіння майном або одержання незаконного доходу іншим шляхом.

Аналіз кримінальних справ показує, що при розслідуванні злочинів, пов'язаних з підробкою та використанням підроблених документів, до кримінальної відповідальності притягаються, як правило, особи, які використовували підроблені документи, тобто скоїли основний злочин шляхом використання підробленого документа [2]. Підроблювачі ж, як правило, для слідства залишаються невідомими. В 74 % кримінальних справ, у випадках групового скоєння злочинів, справи щодо підробки документів виділялися до окремого провадження і слідство призупинялося на підставі того, що особу злочинця не було встановлено. Причинами таких результатів розслідування є передусім психологічне ставлення слідчих до підробки документів, як до незначного злочину, на доказування якого вони не бажають витрачати сили і час. Немалозначним фактором є недостатність знань про способи підробки документів, їх ознак та відсутність навичок використання цієї інформації у розшуковій і слідчій діяльності. Таке ставлення до підробки документів у багатьох випадках є причиною повернення кримінальних справ про економічні злочини на додаткове розслідування.

При розслідуванні підробки документів у сфері економіки слід розрізняти способи підробки документів і способи використання підроблених документів. Ці дві окремі дії часто передбачаються однією статтею КК, але повинні доказуватися окремо. Крім цього, дії з використання підробленого документа можуть охоплюватися об'єктивною стороною окремих економічних злочинів, тоді як підробка документів завжди є окремим складом злочину. Доказування підробки документів і використання підроблених документів має свої відмінності і специфіку, яку треба враховувати при

розслідуванні як основних злочинів, так і підробки документів та їх використання.

Спосіб підробки документа — це сукупність технічних засобів та прийомів, за допомогою яких вносяться зміни до первинного змісту дійсного документа, виготовляється (оформлюється) чи затверджується повністю або частково завідомо неправдивий документ. У зв'язку з різноманіттям у сучасній Україні носіїв інформації, на яких створюються та існують офіційні документи, кожен з яких має свої, притаманні тільки йому властивості, доцільно окремо розглянути способи підробки паперових, електронних і пластикових документів.

При скоєнні злочинів у сфері економіки злочинці поряд з використанням вже відомих і детально описаних у криміналістичній літературі способів підроблення паперових документів (підчистка, витравлення, дописування тощо) винаходять нові, більш досконалі способи. У їх основу покладено використання досягнень сучасної науки і техніки, до яких належать комп'ютери і периферія (сканер, принтер), копіювально-розмножувальні апарати, факси [7]. Особливості зазначених технічних засобів впливають на тактику проведення окремих слідчих дій, призначення і проведення експертних досліджень і доказування економічних злочинів.

Зустрічаються також і випадки підробки відбитків печаток і штампів за допомогою сучасної копіювально-розмножувальної техніки, а також виготовлення печаток і штампів як кустарним, так і виробничим способом (за підробленими заявками). Слід зауважити, що в документообігу України використовуються два різновиди бланків: фірмові та бланки суворої звітності. Якщо фірмові бланки проектуються та виготовляються суб'єктами підприємництва або за їх ініціативою іншими суб'єктами підприємництва, то бланки суворої звітності виготовляються лише за державним замовленням на фабриках Держзнаку України і мають відповідати визначеним вимогам щодо їх виготовлення, використання та зберігання. Поширеною є і підробка підписів, як традиційна, так і з використанням сучасних технологій (сканування з наступним роздрукуванням).

Способи підробки електронних документів часто пов'язані з несанкціонованим доступом до комп'ютерних систем. Наприклад, закордонна практика свідчить, що понад 80 % злочинів з використанням підроблених електронних документів скоюються співробітниками компаній та банків, які мають доступ до комп'ютерних мереж та систем, або особами, які раніше працювали на такі компанії (так званими "інсайдерами") [8].

Підробка електронного документа здійснюється шляхом створення або оформлення заздалегідь неправдивого електронного документа з подальшим його введенням до електронного документообігу компанії чи системи електронних платежів. Випадки внесення змін до офіційного електронного документа нам не відомі, хоча повністю виключити їх існування неможливо, незважаючи на складність процедури підробки. Внесення змін до електронного документа потребує глибоких знань із програмування, оскільки для отримання доступу до змісту електронного документа необхідно отримати несанкціонований доступ до системи документообігу, яка, як правило, захищена, а після цього розкодувати сам документ, тобто підібрати електронно-цифровий підпис, після чого закодувати його цим самим ключем-програмою. При виявленні і доказуванні способу підробки електронного документа слід враховувати особливості програмного забезпечення, яке використовується для функціонування електронного документообігу та забезпечення доступу до нього, а також особливості сертифікатів відкритого і закритого ключів електронного цифрового підпису.

Практика правоохоронних органів України і зарубіжний досвід свідчить про появу та інтенсивне зростання кількості випадків інтелектуальної підробки та злочинного використання електронних документів. Наприклад, використання неправдивих міжбанківських розрахункових документів з метою заволодіння чужим майном, фальсифікація співробітниками банків внутрішніх банківських документів з метою поповнення власного рахунка, генерація заздалегідь неправдивих електронних розрахункових документів, придбання товарів у мережі Інтернет з використанням викрадених чужих номерів банківських платіжних карток тощо [3, *105*].

Підробка банківських пластикових карток, яка є дуже розповсюдженою у країнах з розвиненими системами електронних платежів, набуває зростання і в Україні. Застосування пластикових карток в Україні збільшується у геометричній прогресії, разом з випадками їх підробки та шахрайського використання [4].

Способи підробки пластикових карток можна розділити на дві великі групи: 1) підробка дійсної картки; 2) виготовлення фальшивої картки.

Підробка дійсної картки — це фізична зміна інформації на поверхні картки та перекодування електронної інформації на магнітній стрічці з на-

ступним її використанням. З цією метою використовуються викрадені, знайдені або власні картки.

Зміна інформації на поверхні картки шляхом перебивання рельєфних зображень або заміни підпису держателя на поверхні картки полягає у зміні вибитих рельєфних зображень цифр та букв на пластикові. Зміни на поверхні картки вносяться шляхом замазування чужого підпису білою фарбою або заклеювання смужкою білого паперу і нанесення підпису іншої особи. Зміна інформації на пластикові проводиться за допомогою термообробки — нагрівання картки з попереднім зрізанням бритвою або затиранням пемзою літер та цифр із заміною їх на нові, шляхом наклеювання на картку плівки з нанесеними реквізитами з подальшим видавленням написів.

Перекодування магнітної стрічки являє собою зміну інформації, яка в ній міститься. Цей спосіб є більш складним і потребує більш досконалого та дорогого обладнання. З цією метою використовується спеціальний прилад — декодер, який при з'єднанні з комп'ютером зчитує та розкодовує інформацію, яка міститься на магнітній стрічці. За його допомогою також можливо внести нову інформацію до магнітної стрічки. Особливостями цього способу є те, що злочинці використовують не лише викрадені або загублені картки а й свої особисті. Як правило, такі картки використовуються під час розрахунків за речі та послуги. При використанні такої картки всі зовнішні риси не змінені і тому вона не викликає підозри у продавця. Хоча, згідно з інструкціями, продавець при прийнятті такої картки до платежу зобов'язаний звірити інформацію на магнітній стрічці, яка друкується касовим апаратом на сліпі, з інформацією на поверхні картки, але вони не завжди це роблять, оскільки вступають у змову зі злочинцями.

Другим способом підробки є повне виготовлення фальшивої картки, так зване шахрайство "білого пластику". Полягає він у виготовленні картки з використанням чистого шматка пластику, на який наносяться всі необхідні реквізити, включаючи магнітну стрічку, на зразок якої, як правило, використовується відеоплівка. Така картка зовні виглядає як справжня і приймається як до сплати в крамницях, так і банкоматом для отримання готівки. Повне виготовлення фальшивої картки має дві форми: а) виготовлення фальшивої картки, яка не існувала і не випускалася банківською установою; б) виготовлення дублікату існуючої картки, який забезпечує доступ до чужого банківського рахунка, так зване клонування карток.

Виготовлення фальшивої картки має свої особливості, які полягають у тому, що злочинці використовують реквізити картки, які були згенеровані спеціальними програмними засобами. За останніми дослідженнями 15 спроб достатньо для того, щоб згенерувати номер банківської картки. Така генерація номера картки є можливою, оскільки в її процесі використовуються певні математичні алгоритми перетворення номера банківського рахунка держателя картки, який може бути отриманий за допомогою корумпованого співробітника банку. Такі програми, які працюють за алгоритмами банківського програмного забезпечення, що генерує номери платіжних карток, можна придбати навіть в Інтернеті. Світовій практиці відомі також випадки, коли співробітники банків повідомляли злочинцям номери банківських карток, які ще не були емітовані. Виготовлення дублікату картки полягає у копіюванні на незаконно придбану картку або власну картку злочинця інформацію про картку і банківський рахунок іншої особи, а також повне виготовлення дублікату картки іншої, як правило, заможної особи.

Найбільш якісні підроблені картки до останнього часу виготовлялися злочинним угрупованнями країн Південно-Східної Азії. На сьогодні світові експерти найякіснішими підробками вважають картки, виготовлені на території країн СНД.

Окремим різновидом злочинної діяльності, пов'язаної з підробкою банківських карток, є незаконне заволодіння інформацією про реквізити картки, які в подальшому використовуються для підробки дійсних і виготовлення фальшивих карток. На сьогодні існує кілька способів отримання такої інформації, серед яких: 1) "скіммінг" — незаконне копіювання інформації, яка міститься на магнітній стрічці під час розрахунків з використанням картки (в готелях, ресторанах, крамницях); 2) несанкціонований доступ до баз даних банківських установ і підприємств, в яких міститься інформація про реквізити карток; 3) незаконне встановлення в банкоматах обладнання для копіювання інформації з магнітної стрічки картки і підглядування персонального ідентифікаційного коду/встановлення несанкціонованих банкоматів; 4) отримання інформації шляхом дослідження сміття в офісах і помешканнях осіб; 5) отримання такої інформації шляхом обману.

"Скіммінг" є найпоширенішим способом заволодіння інформацією про реквізити банківської пластикової картки. Полягає він у незаконному

копіюванні співробітником ресторану, готелю або крамниці інформації на магнітній стрічці картки. Коли клієнт розраховується, він передає картку офіціантові чи іншій особі, яка приймає її для оплати. Під час зняття інформації з магнітної стрічки в спеціальному терміналі для виготовлення сліпу (чека), особа копіює зміст магнітної стрічки на власний пристрій, так званий "скіммер". Сучасні "скіммери" мають розмір сірникової коробки і можуть вміщати до 200 номерів карток. Така операція займає 1–2 секунди. В Україні "скіммінг" поширений в основному в м. Києві, як правило, в дорогих ресторанах, розташованих у центрі міста. Потерпілими в основному стають іноземці, які розраховувалися з використанням карток. На цьому виді злочинної діяльності спеціалізуються організовані злочинні групи, які мають міжнародні зв'язки.

Несанкціонований доступ до баз даних банківських установ підприємств та Інтернет-крамниць здійснюється хакерами з використанням всесвітньої інформаційної мережі Інтернет. У подальшому викрадена таким чином інформація використовується для продажу реквізитів карток у мережі Інтернет, ціна на які сягає від 40 центів до 5 доларів США, залежно від ступеня захищеності картки і, відповідно, до суми грошей, яку можна отримати. Були випадки, коли хакери вимагали від керівництва підприємств та крамниць великі суми грошей, погрожуючи розмістити інформацію, викрадену з їх баз даних, в Інтернеті. Останнім часом хакери з України і Росії вважаються найкваліфікованішими у цій сфері. За даними американської газети "Нью-Йорк Таймс", Україна має найбільший у світі ринок збуту реквізитів чужих пластикових карток, які згодом використовуються для виготовлення підроблених карток, та для купівлі товарів за допомогою всесвітньої мережі Інтернет [6].

Незаконне встановлення в банкоматах обладнання для копіювання інформації з магнітної стрічки картки і підглядування персонального ідентифікаційного коду/встановлення несанкціонованих банкоматів є не дуже розповсюдженим, але достатньо ефективним способом заволодіння інформацією про реквізити банківських карток. У Франції і Великобританії були зафіксовані випадки встановлення несанкціонованих банкоматів, які були оснащені обладнанням, необхідним для копіювання інформації. Встановлення в банкоматах обладнання для копіювання інформації з магнітної стрічки неодноразово мало місце як у країнах Заходу, так і в Росії. Наприклад, у Москві була затримана група студентів, які виготовили спеціальний пристрій, що був прикріплений до банкомату в місці, куди вставляється картка, а спеціальна відеокамера записувала персональний ідентифікаційний номер. Спеціальний пристрій надійно кріпився до банкомату і був пофарбований у його колір. Після отримання іформації про картку злочинці виготовляли дублікат картки і отримували безмежний доступ до рахунка. В результаті цієї злочинної діяльності постраждало близько 200 осіб, а злочинці заволоділи грошовими коштами на загальну суму 700 тис. дол. США [8].

Отримання інформації шляхом аналізу сміття поширене в країнах з розвиненою економічною інфраструктурою. Полягає він у аналізі всіх паперів, які викидаються тією або іншою особою. Особливу увагу злочинці звертають на сліпи — чеки, вибиті на спеціальному терміналі в результаті розрахунку з використанням пластикової картки або з банкомату про залишок коштів на рахунку, звіти з банку про стан рахунка особи і листи, в яких повідомляється персональний ідентифікаційний номер картки, персональні дані про особу, які вимагають банки при відкритті рахунка тощо. У результаті таких дій злочинці отримують інформацію про номер банківського рахунка, реквізити банківської картки, поштову адресу і коди особи, які в подальшому використовуються для підробки та незаконного отримання банківських карток. Останнє має місце, коли злочинці, які володіють достатньою іформацією особистого характеру, з'являються до банку потерпілого з заявою про втрату картки та/або зміну поштової адреси з проханням надіслати нову картку за новою адресою; або до іншого банку з заявою про відкриття карткового рахунка, використовуючи інформацію з кредитної справи потерпілої особи.

Отримання інформації про особу шляхом обману має місце, коли до особи телефонують або надсилають листи від імені банку або іншої фінансової кредитної установи з проханням підтвердити ті або інші дані про особу, які були начебто втрачені/перекручені в результаті певних збоїв у роботі банку чи іншої установи.

Таким чином, зазначені способи підробки документів застосовуються з метою створення можливості або сприятливих умов для скоєння предикатних злочинів. Характерною рисою підробки документів у сфері економіки є те, що разом з підробленими використовуються також чужі документи, тобто справжні документи, власниками яких є інші особи.

Література

1. *Кримінальний* кодекс України від 05.02.2003 р. // Голос України. — 2003. — 12–13 берез.

2. *Белкин Р. С.* Курс криминалистики: Учеб. пособие для вузов. — 3-е изд., доп. — М., 2009. — 620 с.

3. *Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін.* Комп'ютерна злочинність: Навч. посіб. — К.: Атіка, 2008. — 240 с.

4. *Вертузаєв М. С., Кондратьєв Ю. А. та ін.* Способи здійснення злочинів з використанням банківських платіжних карт // Інформаційні технології та захист інформації. — Запоріжжя, 2009. — С . 51.

5. *Клименко Н. І.* Проблеми посилення боротьби з економічною злочинністю в Україні // Державно-правова реформа в Україні: Матеріали наук.-практ. конф. — К., 2007. — С. 292.

6. *Турчинов О.* Тіньова економіка і тіньова політика // Політ. думка. — 2006. — № 3–4. — С. 76.

7. *Шепітько В. Ю.* Злочини в сфері економіки: сучасні проблеми криміналістичної науки // Вісн. Акад. правових наук. — Харків: Право, 2007. — С. 160.

8. *Credit* Card Theft Thrives Online as a Global Market // New York Times. — 2002. — May 13.

Обґрунтовується, що при скоєнні економічних злочинів, які є основою злочинних технологій збагачення, документи стають предметами посягання з метою їх подальшого використання як засіб підготовки та скоєння злочину, а властивості підробленого документа мають вплив на умови та характер їх використання. У механізмі злочинних технологій збагачення неправдиві документи виступають єдиним або найпоширенішим засобом досягнення злочинної мети — незаконного заволодіння майном або одержання незаконного доходу іншим шляхом.

Обосновывается, что при совершении экономических преступлений, которые являются основой преступных технологий обогащения, документы становятся предметами посягательства с целью их дальнейшего использования в качестве средства подготовки и совершения преступления, а свойства подделанного документа влияют на условия и характер их использования. В механизме преступных технологий обогащения неправдивые документы выступают единым или наиболее распространенным средством достижения преступной цели — незаконного овладения имуществом или получение незаконного дохода другим путем.

In the article the author proves that the economic crimes that are the basis of criminal enrichment technology, the documents become the subject of abuse for their subsequent use as a means of preparing and committing a crime, and the properties of forged documents have an impact on the environment and the nature of their use. In the mechanism of criminal enrichment technology untrue documents act as one or the most common means of criminal purpose — the illegal acquisition of property or obtaining illegal income in another way.

Надійшла 8 листопада 2010 р.