РОЗКРАДАННЯ БЕЗГОТІВКОВИХ ГРОШОВИХ КОШТІВ БАНКУ З ВИКОРИСТАННЯМ ФІКТИВНИХ РОЗРАХУНКОВИХ ТЕХНОЛОГІЙ

Корнієнко В.В.,
кандидат юридичних наук, старший викладач кафедри криміналістики та судової експертології
Харківського національного університету внутрішніх справ

Для успішної боротьби з розкраданнями безготівкових грошових коштів, що знаходяться на рахунках клієнтів банку, треба добре орієнтуватися у технології фінансових розрахунків. Безготівкові платежі між суб'єктами підприємницької діяльності здебільшого не можуть бути завершені в межах одного банку. Усі розрахунки за угодами суб'єктів підприємницької діяльності, які обслуговуються різними банками є міжбанківськими розрахунками. Останні являють собою систему організації та здійснення платежів за грошовими вимогами та зобов'язаннями, що виникають між банківськими установами.

Платіжно-розрахункова функція банків нарівні з прийняттям депозитів і наданням позик належить до найважливіших банківських операцій. На здійснення розрахунків витрачається не менше двох третин операційного часу банківського персоналу. До масштабної перебудови платіжно-розрахункової системи в Україні (1992-1994 рр.) між установами колишнього Держбанку СРСР міжбанківські розрахунки здійснювалися за системою міжфіліальних оборотів (МФО), яка була запроваджена в 1933 році. Розрахунки через систему МФО здійснювалися переказуванням сум за рахунками у різних установах однієї системи банку. В МФО брали участь усі філії банку, однак у кожній конкретній операції - дві філії, що кореспондували між собою. Одна з них видавала доручення, тобто починала операцію і здійснювала початковий

провід. Друга виконувала доручення та відповідала першій, виконуючи відповідний оборот.

Наразі запроваджено автоматизовану систему міжбанківських розрахунків з використанням прогресивних комп'ютерних технологій (система Клієнт-банк, Інтернет-банкінг, карткове обслуговування, і доступ до міжнародних платіжних систем SWIFT, VISA тощо). Міжнародні банківські системи зв'язані між собою мережею кореспондуючих рахунків типу «Лоро» та «Ностра». Сучасні електронні банківські технології майже витіснили з обігу документарну форму, в якої відображаються бухгалтерські проводки за операціями банку. Електронний документообіг та миттєвість платежів за умов повної автоматизації процесів все ж таки послаблюють контроль за цим напрямком, що значно полегшує здійснення різного роду зловживань. Електронний вигляд документів, з притаманними їм атрибутами, видається більш уразливим для різного роду підробок і маскування слідів злочину. А це ускладнює пошук криміналістично значимої інформації.

Так зване комп'ютерне моделювання в структурі технології розкрадання безготівкових грошей з використанням програмного устаткування – це комплекс способів, що одночасно застосовуються для ухилення від оподаткування і розкрадання коштів, виведених за баланс фінансової звітності банку. Комп'ютерна програмна оболонка включає відповідні технології ведення подвійної бухгалтерії (легальної і тіньової), яка заснована на існуванні в електронній мережі банку чи підприємства двох одночасно діючих програм автоматизованого бухгалтерського обліку із взаємопов'язаними контрольними даними. Використання цієї моделі характерно також для банків, які іноді з метою ухилення від оподаткування створюють поза балансом фінансово-господарської діяльності тіньові кредитні портфелі, що передбачають здійснення в «тіні» як пасивних, так і активних операцій з повним їх оформленням на рівні легітимних операцій. Всі співробітники банку, які за природою своїх операційних службових функцій включені у складні схеми

виводу в «тінь» значних сум коштів, розуміють реальний зміст і протиправний характер таких операцій.

З кримінально-правової точки зору у технології розкрадання безготівкових грошових коштів клієнтів банку з використанням фіктивних розрахункових документів та комп'ютерних програм основними злочинами, що безпосередньо направлені на незаконне одержання грошових коштів, як правило, виступають: розкрадання безготівкових грошових коштів клієнтів банку з використанням службового становища осіб, які мають доступ до рахунків (ч.2 ст. 191 КК України) та розкрадання коштів за допомогою шахрайських дій (ст. 190 КК України). Найбільш типовими злочинними цілями, для досягнення яких неправомірно використовуються комп'ютерна техніка, є підробка рахунків і платіжних відомостей, фальсифікація платіжних документів, тощо.

На шляху до злочинної мети вчиняється низка допоміжних (проміжних, додаткових) злочинів: незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків (ст. 200 КК України); незаконне використання електронно-обчислювальної техніки (комп'ютерних мереж та програмного забезпечення) ст.ст. 361-363[1] КК України) підробка документів, службове підроблення (ст.ст. 357, 358, 366 КК України), посадові злочини (ст.ст. 364-368) та ін. З метою приховування ознак фіктивності операцій, вони не відображаються у документах аналітичного та синтетичного фінансового обліку. Тобто не робляться відмітки про операцію в особистих рахунках юридичних (або фізичних) осіб, не вносяться дані у бухгалтерський журнал реєстрації операцій дня, зведені карточки і щоденні перевірочні відомості, що також не знаходить своє підтвердження у щоденному балансі, який банки надсилають до Національного банку України.

Найбільш типово злочинна схема виглядає так. Відповідна особа чи група осіб акумулює суму в безготівковому вигляді для наступного її вилучення з поточного чи кореспондентського рахунку. На цій стадії

зловмисники проводять необхідні операції з програмним забезпеченням в цілях отримання можливості введення відповідних помилкових даних. Тут поєднуються дії по підготовці злочину і приховання його слідів. Як зазначає в своєму спеціальному дослідженні В.Д. Поливанюк, відстежити подібні махінації буває достатньо складно, особливо коли в програму вносяться тимчасові зміни, що автоматично усуваються після виконання необхідних незаконних операцій. Зміна даних може бути проведена шляхом введення в комп'ютерну банківську систему сум, які реально на даний рахунок не зараховувалися, внесення поправок при нарахуванні відсотків і т.д. [2, с. 10].

Якщо при цьому працівник банку використовував чужі рахунки, то після утворення зайвих сум, він переводив їх на свій єдиний рахунок або розкидав по декількох рахунках, відкритих на вигадані імена. Злочинна акція закінчується зняттям необхідної інформації або грошей з електронних рахунків клієнтів банку, їхнього безпосереднього присвоєння або переказу на рахунки фіктивних фірм.

Приховання злочинних дій відбувається шляхом відновлення початкової програми, що зазнала змін в процесі неправомірного доступу до банківської мережі. Це звичайно буває під силу тільки фахівцям дуже високої кваліфікації і ступеня доступу до банківського програмного забезпечення.

Можна зробити висновок, що успішній протидії розглянутої технології протиправного збагачення стає брак досвіду слідчих у викритті таких дій, латентний характер здійснення злочинних втручань у діяльність програмного забезпечення, а також можливість швидкого знищення слідів. Керівництво банків природно не квапиться повідомляти правоохоронні органи, виявивши факти зловживань з боку своїх працівників, бажаючи владнати все своїми силами.

Слід також звернути увагу, що під час кримінальних проваджень у досліджуваній сфері мають місце складності в розмежуванні закінченого злочину і замаху. Це відбувається в тих випадках, коли, наприклад, оперативні працівники проводять затримання ймовірних розкрадачів до проведення ними

операцій з грошима, переведеними на рахунки по підробленим документам. Нерідко така невчасність згодом ускладнює роботу слідчого по встановленню попередньої змови затриманих розкрадачів на організацію привласнення перерахованих коштів, розподілу ролей, встановленню кому і на скільки спричинено збитків і т.д.

Література:

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III [Електронний ресурс] // Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14

2. Поливанюк В. Д. Криміналістична характеристика злочинів, вчинених у банківській системі з використанням сучасних інформаційних технологій. [Електронний ресурс] / В. Д. Поливанюк // Режим доступу: http://www.crime-research.iatp.org.ua/library/Polivan.htm

3. Попович І. І. Криміналістичне забезпечення обігу розрахункових документів у банківській системі з метою запобігання вчиненню злочинів: автореф. дис. на здобуття наук. ступеня канд. юрид. наук за спец. 12.00.09 «кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / Інна Іванівна Попович; Національний університет внутрішніх справ України, 2007. – 20 с.