УДК 351.745.7:343.9:343.352

Фінагеєв Валерій Олександрович – кандидат юридичних наук, доцент кафедри цивільного права і процесу Національної академії внутрішніх справ

СПОСОБИ ВЧИНЕННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ЗАСОБІВ ДОСТУПУ ДО БАНКІВСЬКИХ РАХУНКІВ

Здійснено огляд та аналіз теоретичних засад і практичних питань методики розслідування злочинів, пов'язаних із незаконним доступом до банківських рахунків. Сформульовано й обґрунтовано низку нових положень і висновків, що мають значення для криміналістичної науки, слідчої та судової практики. Розкрито зміст елементів криміналістичної характеристики злочинів цієї категорії. Виокремлено способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків.

Ключові слова: спосіб; шахрайство; банк; банківська картка; засоби доступу до банківських рахунків.

Криміногенні ознаки економіки України не лише перешкоджають нормальному розвитку фінансової системи країни, а й вимагають підвищення ефективності діяльності правоохоронних органів, пошуку найбільш оптимальних підходів до розв'язання проблем, що виникають під час виявлення та розслідування кримінальних правопорушень у кредитно-фінансовій сфері, зокрема шахрайства з фінансовими ресурсами [1, с. 279].

Більшість шахрайських посягань учиняють групи з чітким розподілом ролей співучасників, які вдаються до хитрощів для обманювання потерпілих (найчастіше це збут підроблених

коштовностей, карткове махлярство, заволодіння цінностями під приводом надання послуг і виконання робіт за різними цивільно-правовими угодами, обман у лотереях, використання підроблених документів, обрахування під час розмінювання грошових купюр, вручення на рахунок оплати так званих «ляльок», гадання, ворожіння, шлюбні афери, видавання шахраями себе за представників органів публічної влади, штатних співробітників відомих комерційних і некомерційних організацій, побудова фінансових та інших «пірамід») [2, с. 109].

Незаконний доступ до банківських рахунків технологічно поєднує пов'язані між собою кримінально карані діяння проти власності (ст. 185, 190, 191 Кримінального кодексу (КК) України), у сфері господарської діяльності (ст. 200, 205, 209, 231 КК України), використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. 361, 361–1, 362 КК України), службової діяльності. Зростає питома вага кримінальних правопорушень, учинених у складі організованих злочинних груп за участі службових осіб банків. Злочинці вміло приховують власні дії, зокрема справжні наміри маскують за допомогою удаваних юридичних угод, а збитки – шляхом підроблення фінансових документів, незаконного втручання в роботу автоматизованих інформаційних систем тощо. Практиці відомо про низку інших проблем збирання доказів, встановлення причетності до них конкретних осіб, проведення процесуальних дій.

До того ж, з прийняттям нового Кримінального процесуального кодексу (КПК) України, порівняно з уже застарілою практикою досудового розслідування, особливого значення набуває удосконалення наявних і створення нових методик виявлення та розслідування злочинів у сфері банківської діяльності. Це, відповідно, потребує формування адаптованої до сучасних вимог методології, упровадження її в практику та акцентування уваги на питаннях організації початкового етапу розслідування, проведення слідчих (розшукових) дій [1, с. 4]. Зазначені обставини зумовлюють актуальність обраної теми.

Загальні положення криміналістичної методики, зокрема щодо протидії виявам економічної злочинності та фінансового шахрайства, розглядали у своїх працях Л. І. Аркуша, В. П. Бахін,

Р. С. Бєлкін, В. В. Бірюков, В. І. Василинчук, А. Ф. Волобуєв, В. І. Галаган, А. В. Іщенко, Н. С. Карпов, В. О. Коновалова, В. В. Лисенко, Є. Д. Лук'янчиков, Г. А. Матусовський, Д. Й. Никифорчук, Ю. Ю. Орлов, В. Л. Ортинський, М. А. Погорецький, Р. Л. Степанюк, В. В. Тіщенко, О. Ю. Татаров, Л. Д. Удалова, К. О. Чаплинський, С. С. Чернявський, В. Ю. Шепітько, О. О. Юхно та ін. Різні аспекти виявлення та розслідування злочинів у банківській сфері висвітлено в дослідженнях О. П. Бущана, В. П. Головіної, В. В. Корнієнка, В. Д. Ларічева, Р. П. Марчука, М. М. Панова, І. М. Осики, Т. А. Пазинич, В. В. Поливанюка, А. В. Реуцького, Л. М. Стрельбицької та ін.

З огляду на зазначене, метою написання статті є висвітлення окремих теоретичних і практичних проблем щодо виявлення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків, а також виокремлення та аналіз певних способів учинення таких злочинів.

Усі способи вчинення зазначених злочинів можна диференціювати на три основні групи: 1) способи незаконного доступу до банківських рахунків, пов'язані з використанням розрахунків платіжними дорученнями; 2) способи вчинення злочинів, пов'язаних із незаконним доступом до банківських рахунків, пов'язані з використанням операцій у сфері обігу банківських платіжних карток; 3) способи вчинення злочинів, пов'язані з використанням інших засобів доступу до банківських рахунків.

1. Способи незаконного доступу до банківських рахунків, пов'язані з використанням розрахунків платіжними дорученнями.

За оцінками експертів банківського сектору, близько 95 % платежів у банківській системі здійснюють із використанням саме платіжних доручень. Поширеність такого платіжного засобу сприяє маскуванню шахрайських операцій у загальному масиві операцій та робить цю форму розрахунків привабливою для злочинців. Способи використання платіжного доручення з метою обману та зловживання довірою можна умовно поділити на три підгрупи.

Перша підгрупа – використання платіжного доручення як фіктивного платіжного інструмента без перерахування коштів.

У разі використання платіжного доручення як фіктивного платіжного інструмента підроблене платіжне доручення використовують для формування в потерпілого переконання, що платіж насправді здійснено.

Загальна схема злочину полягає в тому, що злочинці підроблюють платіжне доручення найчастіше від імені підприємства з ознаками фіктивності (певна фірма відкриває розрахунковий рахунок в банку з мінімальним або нульовим залишком коштів). Потенційний потерпілий (зазвичай постачальник в угоді) не може перевірити реальний стан рахунку контрагента через банк, оскільки ця інформація, згідно із законодавством, є банківською таємницею, охоронюваною законом. Нерідко відкриття рахунку супроводжується активними діями зловмисників, які запевняють потерпілого про очікуване надходження коштів на рахунок (зазвичай повідомляють завідомо неправдиву інформацію про нібито реалізовані ними масштабні угоди).

Подальші дії злочинців передбачають укладання угоди на придбання партії товару на умовах передплати з безготівковою сплатою всієї вартості придбаного після фактичної поставки товару на склад. Як доказ фіктивного перерахування коштів шахраї демонструють постачальнику останній примірник платіжного доручення з відміткою банку про прийняття розрахункового документа для виконання.

Застосування цієї схеми нерідко пов’язано з попередніми діями злочинців, які мають на меті переконати потерпілих у власних «добрих» намірах. Шахраї укладають першу угоду на відносно невелику суму та вчасно її сплачують. Оформлюють платіжні доручення зазвичай у відділенні банку, через який постачальник здійснює розрахунки з іншими клієнтами. Завершальним кроком є придбання товару на значну суму та пред’явлення як підтвердження його сплати копії підробленого платіжного доручення. У разі, якщо товар одержує безпосередній учасник розкрадання, крім підробленого платіжного доручення, пред’являють підроблені паспорти та довіреності на одержання товару.

Друга підгрупа – використання підробленого платіжного доручення для заволодіння грошовими коштами суб’єкта

господарювання шляхом їх перерахування з банківського рахунку цієї організації на інші рахунки.

У разі використання підробленого платіжного доручення для розкрадання грошових коштів суб'єкта господарювання шляхом їх перерахування з рахунку організації на інші рахунки банку направляють підроблені платіжні документи. Як підставу для сплати платіжними дорученнями виготовляють фіктивний договір. Нерідко злочини вчиняють за участі працівників банку. Викрадені в такий спосіб кошти переводять на рахунки спеціально створених (підібраних) фіктивних фірм, а зрештою – перетворюють на готівку та привласнюють. Важливим для цієї групи способів є те, що злочинці, як правило, володіють інформацією про реквізити розрахункових рахунків і специфіку фінансової діяльності організації, на яку спрямоване посягання.

Здебільшого такі посягання вчиняють за участі бухгалтерських працівників безпосередньо організації або банку, у якому відкрито рахунки суб'єкта господарювання, шляхом матеріального й інтелектуального підроблення платіжних документів суб'єкта господарювання (характерно для всіх «зовнішніх» розкрадань) або з використанням доступу до систем електронних платежів та комп'ютерних мереж банку (характерно для «внутрішніх» розкрадань).

Якщо розрахунки платіжними дорученнями здійснюють в електронній формі, для виготовлення такого платіжного документа використовують справжній аналог електронного цифрового підпису, викрадений злочинцями чи переданий їм. Розкрадання коштів шляхом передачі електронною системою платежів «клієнт-банк» підроблених платіжних доручень на цей час набули значного поширення.

В окремих випадках із метою заволодіння коштами суб'єктів господарювання, зокрема державних установ, шахраї використовують «підставних осіб», які не завжди обізнані із загальною злочинною схемою. На роль таких технічних виконавців організатори злочину добирають осіб із представників малозабезпечених верств населення (пенсіонерів, інвалідів, безробітних, студентів, іноземців), громадян, які не мають

постійної роботи та певного місця проживання, ведуть аморальний спосіб життя, психічно хворих тощо.

Третя підгрупа – використання підроблених платіжних доручень для розкрадання коштів безпосередньо в банку.

Підроблені платіжні доручення для розкрадання коштів безпосередньо в банку використовують переважно банківські працівники. Виявом шахрайства вважається несанкціоноване списання коштів платника (потерпілого) на розрахунковий рахунок співучасника злочину.

Для виготовлення підроблених платіжних доручень на паперових носіях в окремих випадках виготовляють підроблені відбитки печаток (з підробленим кліше або шляхом сканування). Зазвичай використовують справжні печатки, якими тимчасово заволоділи. Підроблюють підписи уповноважених працівників банку. Електронні копії платіжних доручень можуть завіряти електронними аналогами підпису, носії яких тимчасово вилучені із законного володіння або викрадені в уповноважених осіб.

2. Способи вчинення злочинів, пов'язані з використанням операцій у сфері обігу банківських платіжних карток.

В основу розподілу способів цієї групи слід покласти такі варіанти реалізації злочинного наміру: 1) незаконне використання справжніх або використання підроблених банківських платіжних карток через мережу банкоматів і платіжних терміналів; 2) втручання в комп'ютерні мережі банку (внесення змін до інформаційних систем і баз даних) з метою незаконного доступу до «карткових» рахунків.

Способи вчинення злочинів, пов'язаних із використанням банківських платіжних карток, мають такі форми вияву: 1) незаконне використання справжньої чужої (вкраденої, загубленої, отриманої шляхом обману, за підробленими документами) картки без внесення до неї змін; 2) використання підробленої картки; 3) незаконне використання реквізитів банківської картки.

Незаконне використання справжньої чужої картки, відповідно, має три різновиди, що залежать від способу одержання картки, повноти інформації щодо картки та наявності співучасників: 1) шляхом втручання в роботу банкоматів; 2) шляхом надання

картки для сплати в торговельній організації чи касі банківської установи; 3) шляхом комбінування зазначених способів.

Втручання в роботу банкомату передбачає використання чужих карток за умов, що злочинець має картку та ПІН-код. Застосування банкоматів є найбільш безпечним способом використання чужої картки, що «працює» доти, доки на картковому рахунку є гроші або доки картку не буде заблоковано банком. Нині спостерігається різке збільшення випадків шахрайства з використанням банкоматів [4, с. 54].

У разі заволодіння карткою без ПІН-коду її використовують у місцях, обладнаних платіжними терміналами, у яких для ідентифікації власника картки порівнюють підпис на зворотній стороні картки та підпис, який залишає покупець на сліпі під час розрахунку в присутності продавця.

У разі використання карток, отриманих належним чином, але за чужими документами, злочинці, як правило, звертаються із заявами до банку про одержання кредитних карток, що використовують для купівлі товарів чи зняття готівки. Усі витрати в цьому разі покриває банк, ураховуючи повернення грошей і відсотків за кредит.

Використання підробленої картки за своєю сутністю не відрізняється від попереднього способу. Єдиною особливістю є те, що в цьому разі злочинці використовують картки, на яких інформацію змінено як фізичними, так й електронними засобами, а також повністю виготовлені картки, у їх числі дублікати реальних карток, емітованих закордонними банками. Ці дії вчиняють здебільшого організовані злочинні групи, до яких належать особи, котрі підроблюють картки, керують діями осіб, які використовують підроблені картки, працівники банків і магазинів, котрі приймають картки до сплати.

Слідчій практиці відомі випадки використання підроблених карток у вигляді дублікатів реально емітованих карток, дані яких використовували під час підроблення.

Незаконне використання реквізитів банківських платіжних карток може набувати двох форм: 1) коли використовують систему розрахунків, під час яких картку не пред’являють, а повідомляють лише її реквізити – номер картки, дату, до якої вона чинна, ім’я та

адресу власника; 2) коли наявне місце зловживання на етапі оформлення розрахунку з використанням картки.

Реквізити чужих карток у разі фізичної відсутності картки використовують під час придбання товарів у мережі Інтернет або за телефоном. Злочинці повідомляють реквізити чужої картки торговельній установі, що стягує кошти з наданого карткового рахунку як оплату за товар і доставляє товари за вказаною шахраєм адресою. Потерпілими в разі застосування такого способу шахрайства стають торговельні установи, що відправляють товар замовникові, а коштів не отримують, оскільки банки або зупиняють операції за рахунком, або відкликають кошти, коли клієнт повідомив про несанкціоноване використання картки.

Зловживання на певному етапі оформлення розрахунку з використанням картки вчиняють продавці або касири шляхом підроблення сліпів із подальшим пересиланням їх до банку та стягненням коштів із рахунку держателя картки за товар, придбаний злочинцями. Вирізняють два види цього способу використання реквізитів картки: 1) шахрайські дії з використанням підроблених сліпів; 2) використання фіктивних підприємств для обслуговування банківських платіжних засобів.

Підроблені сліпи виготовляють вручну без застосування картки шляхом внесення до бланку сліпа необхідної інформації, зокрема реквізитів картки, якими володіють злочинці. Унаслідок цього підроблені сліпи передають банкові для оплати, гроші списують із рахунку держателя картки, чиї реквізити використовувалися, а злочинці отримують товар, який згодом збувають.

Різновидом цього способу є повторне проведення картки через термінал або імпринтер під час розрахунку непомітно для держателя картки. Унаслідок цих дій сума з рахунку держателя стягується двічі: один – за реально придбаний ним товар, другий – за товар або готівку, які вилучають злочинці на суму, сплачену держателем картки за його товар. До такого виду шахрайства вдаються продавці або касири торговельних закладів, обладнаних імпринтерами або електронними терміналами для прийняття банківських карток до сплати.

Характерною рисою таких зловживань є те, що злочинці звертаються до банків від імені суб'єктів підприємництва, яких насправді не існує.

Способи зловживання службовим становищем і неправомірного втручання в комп'ютерні мережі банку задля незаконного доступу до «карткових» рахунків та операцій із використанням платіжних карток.

Характерним прикладом такої комбінації способів незаконного доступу до банківських рахунків є зловживання працівників банків, які, маючи доступ до автоматизованих інформаційних систем і комп'ютерних мереж фінансової установи, здійснюють неправомірний доступ до «карткових» рахунків.

Залежно від умов, за якими здійснюються платіжні операції з використанням банківських платіжних карток, можуть застосовуватися дебетова, дебетово-кредитна та кредитна платіжні схеми. Дебетова схема передбачає здійснення користувачем платіжних операцій із використанням спеціального платіжного засобу в межах залишку коштів, що обліковуються на його рахунку. Під час застосування дебетово-кредитної схеми користувач здійснює платіжні операції з використанням спеціального платіжного засобу в межах залишку коштів, які обліковують на його рахунку, а в разі їх недостатності або відсутності – за рахунок наданого банком кредиту (абз. 2 п. 3.2 гл. 3 Постанови Правління Національного банку України «Про здійснення операцій з використанням спеціальних платіжних засобів» від 30 квітня 2010 р. № 223) [5].

Певну специфіку вчинення незаконного доступу до банківських рахунків має використання зловмисником операцій з кредитними платіжними картками (кредитна схема передбачає здійснення користувачем платіжних операцій із використанням спеціального платіжного засобу за рахунок коштів, наданих йому банком у кредит або в межах кредитної лінії). Особливістю банківської кредитної картки є відкриття банком кредитної лінії, що використовується автоматично щоразу, коли купують товар або беруть кредит у грошовій формі.

На території України дозволене приймання готівки через каси уповноважених банків-емітентів за спеціальними платіжними

засобами користувачів, яким емітенти відкрили рахунки, а також через каси небанківських фінансових установ за спеціальними платіжними засобами, що емітовані нерезидентами [6]. З огляду на це, трапляються зловживання касирів банків із коштами, які приймають від клієнтів для поповнення «карткових» рахунків.

Найменш «кваліфіковані» способи незаконного доступу до банківських рахунків полягають у заволодінні працівниками банків коштами на банківських рахунках шляхом таємного вилучення платіжних карток, що належать (відкриті на ім'я) клієнтам банку.

3. Способи вчинення злочинів, пов'язані з використанням інших засобів доступу до банківських рахунків.

До платіжних засобів, крім документів на переказ і платіжних карток, належать також інші засоби доступу до банківських рахунків, тобто засоби певної форми в паперовому, електронному чи іншому вигляді носія інформації, використання яких ініціює переказ грошей із відповідного рахунка платника. Аналіз нормативно-правових актів у сфері обігу банківських платіжних засобів та судової практики дає підстави для висновку про те, що іншими засобами доступу до банківських рахунків слід визнати, зокрема: грошові та розрахункові чеки; акредитиви; електронні розрахункові документи.

Способи вчинення злочинів, що вчиняються в разі розрахунків акредитивами. Такі злочини пов'язані з наданням неправдивих відомостей про виконання основного договору. Способи їх учинення передбачають переважно обман і зловживання довірою (шахрайство). За своєю схемою ці дії схожі на згадане нами вище використання платіжного доручення як фіктивного платіжного інструмента без реального перерахування грошових коштів: злочинець, діючи від імені певної організації (найчастіше підприємства з ознаками фіктивності), відкриває розрахунковий рахунок в одному з банків, а згодом пропонує покупцеві здійснити постачання певних товарів з оплатою за акредитивом (ця форма розрахунків певною мірою підвищує ступінь довіри до шахрая). Після укладання угоди й одержання від виконуючого банку відомостей щодо відкриття акредитиву шахраї надають до банку підроблені документи про виконання зобов'язань, а також паспорти

на ім'я особи, яка є одержувачем коштів за акредитивом, а в окремих випадках – підроблену довіреність. Обумовлений договором товар покупцеві насправді не надходить.

Способи вчинення злочинів у разі розрахунків чеками. Поняття «чек» передбачає два різновиди: грошовий чек та розрахунковий. Грошові чеки використовують як засіб розрахунків неторговельного характеру, що фактично є грошовим зобов'язанням чекодавця виплатити зазначену в чеку суму чекодержателеві (власнику) готівкою в банку. На зворотному боці чека зазначають цільове призначення платежу. Банк здійснює реєстрацію виданих клієнтові чеків, які звіряє з номерами чеків, пред'явлених до сплати.

Розрахунковий чек – розрахунковий документ, що містить нічим не обумовлене письмове розпорядження власника рахунку (чекодавця) банку-емітенту, в якому відкрито його рахунок, про сплату чекодержателю зазначеної в чеку суми коштів. Останню знімають із чекового рахунка чекодавця в банку й переказують або безпосередньо видають банком чекодержателю. Чековий рахунок – поточний рахунок у банку, розрахунки за яким здійснюють за допомогою чеків (глава 7 Інструкції про безготівкові розрахунки в Україні в національній валюті, затвердженої Постановою Правління Національного банку України від 21 січня 2004 р. № 22) [7].

Сутність злочинних дій під час операцій із грошовими чеками полягає в одержанні грошей за чеком особою, щодо якої не було розпорядження про сплату взагалі, або в одержанні особою коштів на суму, що перевищує розпорядження чекодавця. Для цього шахраї заздалегідь учиняють низку підготовчих дій, зокрема неправомірно заволодівають чистими бланками чеків або заповненими чеками з подальшим їх підробленням; отримують інформацію про банк, реквізити організації, що має в ньому кошти для сплати за чеком, про кореспондентський рахунок, з якого має бути здійснено платіж; здобувають зразки підпису чекодавця; виготовляють підроблені документи для маскування особи одержувача коштів та інші документи. Фальсифікація чеків може бути частковою (шляхом внесення неправдивої інформації

у справжній чек) та повною (шляхом її зазначення у викраденому чистому бланку).

Способи незаконного доступу до банківських рахунків із використанням електронних розрахункових документів. Безготівкові розрахунки проводить банк на підставі розрахункових документів на паперових носіях чи в електронному вигляді. Електронний розрахунковий документ – документ, інформацію в якому представлено у формі електронних даних, серед іншого відповідні реквізити розрахункового документа, який може бути сформований, переданий, збережений і перетворений на візуальну форму представлення електронними засобами.

Зазвичай доступ до електронних розрахункових документів банку мають уповноважені працівники, на яких покладається ведення рахунків фізичних осіб; організація роботи із залучення вкладів і депозитів населення в національній та іноземній валютах; обслуговування фізичних осіб і здійснення операцій із відкриття, ведення та закриття поточних, депозитних рахунків у національній, іноземній валюті та банківських металах; виконання операцій за дорученням клієнтів відповідно до законодавства України та внутрішніх нормативно-правових актів банку. З метою належного виконання вищевказаних обов'язків працівникам банку надається право доступу до системи електронних платежів та індивідуальні паролі для входження та здійснення змін у системі.

Водночас банки (філії) здійснюють міжбанківський переказ за міжбанківськими електронними розрахунковими документами, які вони формують на підставі паперових розрахункових документів клієнтів, паперових розрахункових документів банку (філії), електронних розрахункових документів, отриманих засобами автоматизованих систем від клієнта – ініціатора переказу, електронних розрахункових документів, отриманих засобами внутрішньобанківської міжфілійної платіжної системи від філії банку; електронних розрахункових документів, автоматично сформованих систем автоматизації банку за умовами договорів або згідно з потребою банку (філії);

електронних розрахункових документів, отриманих засобами інших платіжних систем, телекомунікаційних систем, інших засобів зв'язку за умови забезпечення цілісності та конфіденційності інформації тощо.

Учинення злочинів, пов'язаних із незаконним доступом до банківських рахунків, неможливе без попередньої ретельної підготовки, вивчення обстановки, створення передумов (використання ситуації) для незаконного заволодіння чужими коштами та приховування слідів злочину.

Підготовка до злочину передбачає різні за кримінально-правовими ознаками технології злочинної діяльності. Результати вивчення кримінальних справ (матеріалів кримінальних проваджень) свідчать, що вчинення практично всіх злочинів ретельно готувалося (за винятком випадків заволодіння чужими коштами з використанням банківської платіжної карти, що випадково опинилась у правопорушника).

Технологічно етап підготовки до вчинення незаконного доступу до банківського рахунку може містити в собі: 1) незаконне збирання або використання відомостей, що становлять банківську таємницю; 2) підроблення документів на переказ та інших засобів доступу до банківських рахунків; 3) незаконні дії зі спеціальними платіжними засобами, обладнанням для їх виготовлення.

В окремих випадках ці дії поєднані з незаконним втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем і комп'ютерних мереж банку, змовою на вчинення злочинів між працівниками банківської установи та іншими особами, створенням та використанням суб'єктів господарської діяльності з ознаками фіктивності.

Основний етап злочинної діяльності містить у собі дії, спрямовані на заволодіння коштами клієнтів банківської установи або безпосередньо коштами банку. Кримінально-правова оцінка таких дій передбачає заволодіння чужим майном або придбання права на майно шляхом: обману чи зловживання довірою (шахрайство), привласнення, розтрати майна або

заволодіння ним шляхом зловживання службовим становищем, крадіжки. Приховування злочину передбачає дії, спрямовані на легалізацію (відмивання) доходів, одержаних злочинним шляхом.

На етапі підготовки до злочину злочинці розробляють схему (план) майбутньої операції, уживають організаційних і технічних заходів щодо створення належних умов для успішної реалізації мети злочинної діяльності. Особливість цього етапу – практична невразливість від переслідування правоохоронних органів і служб банківської безпеки, оскільки початковий етап злочинної діяльності зазвичай маскується під правовідносини за участі суб'єктів господарювання, правомірні дії громадян або ж виконання своїх функціональних обов'язків працівниками банку.

У механізмі злочину важливу роль відіграють працівники фінансових установ та державних органів, що беруть участь в операції. Ідеться про вчинення ними корупційних правопорушень та службових злочинів, зокрема зловживання службовим становищем, а також різних видів неправомірних утручань у роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, що сприяють досягненню головної мети.

До підготовчих дій належать також отримання детальної інформації про нормативно-правове регулювання й технологію здійснення банківських операцій, ведення відповідних обліків, правила складання документів, порядок їх заповнення та проходження від виконавця до адресата, порядок застосування пошукових та інформаційних систем, захисту інформації тощо. Важливим також є чинник професійної підготовки злочинців (наявність у них навичок фальсифікації документів, застосовування спеціальних технічних засобів, комп'ютерної техніки (зокрема пристроїв для зчитування інформації та виготовлення банківських платіжних карток).

Підроблення документів на переказ та інших засобів доступу до банківських рахунків полягає як у повному виготовленні фальсифікованих платіжних засобів, так і в частковому підробленні справжніх документів. У таких випадках платіжний документ набуває ознак підробленого як за містом, так

і за формою, що зазвичай становить об'єктивну сторону складів злочинів, передбачених ст. 200, 358, 366 КК України. За своїм змістом фальсифікована інформація підробленого платіжного засобу (документів на переказ чи інших засобів доступу до банківських рахунків) повинна: давати можливість ідентифікувати особу, яка ініціює переказ коштів, як таку, що нібито має на це право (номер банківського рахунка, код банку, прізвище ініціатора переказу тощо); містити в собі певний припис щодо незаконної видачі коштів особі, яка не має на це права, або ініціювання переказу коштів з одного банківського рахунку на інший.

Особливості підроблення платіжних документів в електронній формі пов'язані з тим, що електронний документ – це документ, інформацію в якому зафіксовано у вигляді електронних даних, серед іншого й обов'язкові реквізити документа (ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг») [8]. Такий документ має однакову юридичну силу з паперовим, а відповідний електронний цифровий підпис на ньому (що є обов'язковим реквізитом електронного документа і використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу) – однакове правове значення з відповідним підписом на паперовому носії [9].

Підроблення електронного документа може полягати у фальсифікації його обов'язкових реквізитів (інформації про ініціаторів перерахування грошей, підстав платежу, платників, банків, номерів рахунків, суми грошових коштів, що підлягають перерахуванню, тощо) й електронного цифрового підпису (криптографічного набору електронних даних), який дає змогу ідентифікувати автора електронного документа. Зважаючи на те, що електронний документ не має постійного матеріального носія, ідеться про підроблення лише інформації у вигляді електронних даних. Такі дії, як свідчить судова практика, додатково кваліфікують як несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем,

комп'ютерних мереж чи мереж електрозв'язку, а також несанкціоновані дії з інформацією, що підлягає обробці в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, учинені особою, яка має право доступу до неї, тобто за сукупністю зі злочинами, передбаченими ст. 361, 362 КК України.

Дії правоохоронних органів нерідко ускладнюються тим, що між етапами незаконного доступу до банківських рахунків із використанням електронних платіжних документів й усуненням слідів можуть минати незначні проміжки часу.

Підбиваючи підсумки, слід відзначити, що важливу роль в організації виявлення та розслідування злочинів досліджуваної категорії відіграє правильна оцінка способів їх приховування. Способи приховування злочинів, пов'язаних із незаконним доступом до банківських рахунків, можна умовно поділити на три групи.

1. Приховування злочину шляхом маскування інформації та її носіїв: змінення юридичної адреси та фактичного місця перебування суб'єкта господарювання; переведення працівника на інше місце роботи (до іншого підрозділу, іншої установи); використання підроблених платіжних та інших документів і технологічних помилок для маскування незаконної операції; багаторазовий переказ коштів рахунками, змішування на декількох рахунках легальних коштів і таких, що одержані злочинним шляхом; конвертація та переведення в готівку незаконно здобутих коштів; різні операції з легалізації (відмивання) доходів, одержаних злочинним шляхом.

2. Приховування злочину шляхом знищення інформації та її носіїв: ліквідація підприємств і фінансових установ; знищення предметів і документів (приховане їх втратою, незаконним заволодінням), за допомогою яких було вчинено злочин (платіжні документи, бухгалтерська звітність, записи в системах електронних платежів тощо).

3. Приховування злочину шляхом фальсифікації інформації та/або її носіїв: давання завідомо неправдивих показань; викривлення фінансової, статистичної, технологічної, податкової та іншої документації; погрози, переконання або підкуп працівників банківської безпеки, правоохоронних органів й органів контролю, використання корупційного прикриття та інші прийоми протидії розслідуванню.

Певну специфіку мають способи легалізації (відмивання) коштів, одержаних шляхом незаконного використання інформації про банківські платіжні картки (без ПІН-коду). Отримавши зазначену інформацію, зловмисник використовує її для: протиправного придбання послуг операторів мобільного зв'язку, доступу до мережі Інтернет тощо; користування різноманітними платними сервісами (ігровими ресурсами, інформаційними базами, замовленням товарів (послуг) та ін.); придбання товарів в Інтернет-магазинах, речей на Інтернет-аукціонах тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мудряк Т. О. Криміналістичні проблеми розслідування шахрайства з фінансовими ресурсами та шляхи їх вирішення / Т. О. Мудряк // Порівняльно-аналітичне право. – 2014. – № 1. – С. 279–281.

2. Кришевич О. В. Кримінальна відповідальність за шахрайство, вчинене групою осіб за попередньою домовленістю або організованою групою / О. В. Кришевич // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. – № 1 (34). – С. 109–114.

3. Виявлення та розслідування злочинів, пов'язаних з використанням засобів доступу до банківських рахунків : метод. рек. / [В. О. Фінагеєв, С. С. Чернявський, О. Ю. Татаров та ін.]. – Київ : Нац. акад. внутр. справ, 2013. – 79 с.

4. Організація розслідування злочинів, пов'язаних із заволодінням коштами шляхом утручання в роботу банкоматів : метод. рек. / С. С. Чернявський, О. Ю. Татаров, В. О. Фінагеєв та ін.]. – Київ : Нац. акад. внутр. справ, 2013. – 88 с.

5. Про здійснення операцій з використанням спеціальних платіжних засобів : Постанова Правління Національного банку України від 30 квіт. 2010 р. № 223.

6. Інструкції про ведення касових операцій банками в Україні : Постанова Правління Національного банку України від 1 черв. 2011 р. № 174.

7. Інструкції про безготівкові розрахунки в Україні в національній валюті : Постанова Правління Національного банку України від 21 січ. 2004 р. № 22.

8. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851–IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

9. Кичак В. М. Системи документального електрозв'язку : навч. посіб. / Кичак В. М., Семенова О. О., Семенов А. О. – Вінниця : ВНТУ, 2009. – 159 с.

Финагеев В. А. *– кандидат юридических наук, доцент кафедры гражданского права и процесса Национальной академии внутренних дел*

Способы совершения преступлений, связанных с использованием средств доступа к банковским счетам

Проанализированы теоретические основы, практические вопросы методики расследования преступлений, связанных с незаконным доступом к банковским счетам. Сформулирован и обоснован ряд новых положений и выводов, имеющих значение для криминалистической науки, следственной и судебной практики. Раскрыто содержание элементов криминалистической характеристики преступлений данной категории. Выделены некоторые способы совершения преступлений, связанных с использованием средств доступа к банковским счетам.

Ключевые слова: способ; мошенничество; банк; банковская карточка; средства доступа к банковским счетам.

Valerii Finaheiev *– Ph.D in Law, Associate Professor of the Department of Civil Law and Procedure of the National Academy of Internal Affairs*

Methods of Committing Crimes Related to the Use of Bank Accounts Access

The establishment of Ukraine as an independent state parallel to the processes of formation of the legal system and the development of the market economy has led to the inefficiency of the state regulation of the latter, as well as the emergence of the powerful shadow economy because of significant gaps in legislative and regulatory acts. Today, this problem is exacerbated by the rapid growth of the financial sector, which permeates all spheres of social relations, and existing socio-economic situation in the country, resulting in the increasing number of financial crimes.

The current level of criminalization of economic relations could not help but have a negative impact on the world of banking and with a certain probability we can say that this industry has become highly criminalized. In the globalization of the world economy, taking into account changes in the financial system of Ukraine due to innovations in the legislation and the financial and economic crisis, the internal affairs bodies must oppose new manifestations of crime in the monetary market.

The scope of banking activities has never been left without the attention of criminal structures. In recent decades the forms of fraud associated with the use of telegraph memo, plastic means of payment, signature, electronic securities, virtual Internet-stores have spread in the banking sector. However, the range of contemporary issues to combat fraud in the banking sector in Ukraine today is determined not only by the appearance of many new forms of fraud, but also by changes in the factor complex of this type of crime, its globalization and internationalization, so fraud has become one of the most common types of acquisitive crime. These circumstances explain the relevance of the chosen theme.

This article provides an overview and the analysis of theoretical principles and practical techniques for investigating crimes related to illegal access to bank accounts. The paper has formulated and proved a number of new provisions and findings relevant to forensic science, investigation and litigation. It contains elements of criminological characteristics of crimes in this category. The article has determined some ways of committing crimes related to the use of bank accounts access.

Keywords: method; fraud; bank; bank card; means of bank accounts access.