МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ФАКТІВ НЕСАНКЦІОНОВАНОГО ПЕРЕКАЗУ КОШТІВ З РАХУНКІВ КЛІЄНТІВ БАНКУ, ЯКІ ОБСЛУГОВУЮТЬСЯ ЗА ДОПОМОГОЮ СИСТЕМ ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ

Методичні рекомендації

Харків – 2015

Авторський колектив:

Стреляний В.І. – кандидат юридичних наук, провідний науковий співробітник науково-дослідної лабораторії з проблем протидії злочинності навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції Харківського національного університету внутрішніх справ;

Корнієнко В.В. – кандидат юридичних наук, старший викладач кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ.

Рецензент:

Степанюк Р.Л. - доктор юридичних наук, доцент, начальник кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для підрозділів слідства Харківського національного університету внутрішніх справ.

Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування**:** Методичні рекомендації / В.В. Корнієнко, В.І. Стреляний. – Х., 2015. - 71 с.

У методичних рекомендаціях наведена кримінально-правова та криміналістична характеристика фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування, надані практичні поради щодо ефективного проведення досудового слідства за цим напрямком. Призначені для слідчих, оперативних працівників правоохоронних органів, а також курсантів, студентів, слухачів та ад'юнктів.

ЗМІСТ

ВСТУП

Дослідження доводять, що більш ніж 75% від усіх збитків, заподіяних економічною злочинністю, припадає на сферу діяльності банківських установ. Згідно проведеного аналізу найбільш криміногенними залишаються кредитно-розрахункові операції банків. Злочинні зазіхання на ресурси банків завдають збитків не лише банкам та їх клієнтам, а й негативно впливають на функціонування усієї фінансової системи держави. Більш того, банки є провідним елементом у структурі діяльності, так званих, конвертаційних центрів («конвертів»), що представляють собою сукупність фіктивних та реально діючих суб`єктів підприємництва, мета яких – ухилення від податків та легалізація злочинних доходів. Діяльність зазначених структур характеризується високим рівнем латентності, злагодженою організацією учасників та складністю доказування.

Згідно офіційної статистики МВС України останнім часом поширення набули факти шахрайства з фінансовими ресурсами банків, фіктивного банкрутства банківських установ та незаконних операцій з іноземною валютою. Особливе занепокоєння у правоохоронних органів викликають зловживання посадових осіб банківських установ щодо розкрадання грошей з рахунків клієнтів банку з подальшим переведенням їх на рахунки фіктивних підприємств та подальшою легалізацією через мережу «конвертаційних» центрів. Вказана злочинна схема відбувається за допомогою електронної системи дистанційного банківського обслуговування (Internet-banking, «Клієнт-Банк» тощо), яка потребує удосконалення засобів захисту. Серед основних проблем, які суттєво впливають на боротьбу зі злочинами у сфері електронного обслуговування клієнтів банку можна види літи наступне.

По-перше, це системи і технології у сфері діяльності банків, що неудосконалені з точки зору інформаційної безпеки та захисту даних: 1)

використання користувачами комп'ютерної техніки неліцензійного програмного забезпечення, що з великою долею ймовірності може містити в собі шкідливе програмне забезпечення, яке використовується злочинцями; 2) недостатній захист комп'ютерних мереж та приватних ПК та інше.

По-друге, недостатня урегульованість нормативно-правових документів щодо вимог до захищеності систем дистанційного банківського обслуговування клієнтів. Так, багато вчених сходяться на думці, що законодавством України чітко не визначено поняття ключових термінів «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертерризм», «кіберзброя», а лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерних систем та мереж.

Слід зазначити, що даний напрямок протидії злочинним посяганням на ресурси банку ще залишається недостатньо дослідженим. Зокрема, на перший погляд здається, що крадіжки з рахунків клієнтів банку за допомогою систем дистанційного обслуговування (напр. з банківських кредитних карток) вчиняються злочинцями - «хакерами», які не мають відношення до банківської установи. Дійсно, така практика має місце. Але більш масштабні збитки для кредитно-фінансової установи мають факти, коли до подібних дій причетні представники банків. У цьому випадку і схеми злочинної діяльності більш складні, і виявити такі зловживання досить важко з огляду на закритий характер банківської діяльності та обізнаність злодіїв як якісно сховати сліди злочинів та протидіяти розслідуванню.

Практика вказує, що серед обвинувачених – учасників технологій злочинного збагачення у сфері банківської діяльності за подібними категоріями кримінальних проваджень дуже рідко фігурують представники банківського сектору. Хоча, досить часто, саме завдяки їх безпосередньої участі відбувається процес несанкціонованого доступу до

рахунків клієнтів банку та подальшого розкрадання коштів. З цього приводу переважна більшість (82%) опитаних нами слідчих та оперативних працівників по боротьбі з економічною та організованою злочинністю стверджує, що на практиці довести причетність банківських службовців до подібного роду зловживань вкрай важко[1]. Труднощі, на які посилаються опитані, викликані відсутністю методичних розробок, в яких мають бути розкриті зміст злочинної діяльності працівників банку в структурі технологій злочинного збагачення, особливості розкриття та розслідування комплексу економічних злочинів у цій сфері.

З огляду на вищенаведене, у методичних рекомендаціях запропоновано розглянути наступні питання:

- провести кримінально-правовий та криміналістичний аналіз злочинної діяльності у банківській сфері з точки зору комплексного характеру злочинної поведінки;

- з'ясувати особливості початку кримінального провадження по вказаним категоріям кримінальних справ;

- визначити комплекс перевірочних дій та обставин, які підлягають встановленню на початковому етапі розслідування та деякі інші питання.

Окреслені завдання, на нашу думку, допоможуть слідчим та оперативним працівниками ефективніше протидіяти злочинній діяльності у сфері діяльності банків.

[1] Було проведено опитування 127 слідчих органів внутрішніх справ і прокуратури та 133 оперативних працівників, які брали участь у розкритті та розслідуванні злочинів, що вчинені у сфері банківської діяльності.

1. Загальна характеристика функціонування системи дистанційного банківського обслуговування

Сьогодні ринок банківських продуктів і послуг достатньо насичений та різноманітний. Фінансово-кредитні інститути пропонують клієнтам широкий спектр банківських продуктів і послуг. Проте на порядку денному банку завжди гостро стоїть питання про налагодження зручних та ефективних каналів дистрибуції (надання) своїх послуг споживачам.

В умовах жорсткої конкуренції банки просто вимушені не тільки розширювати перелік своїх фінансових та інформаційних продуктів і послуг, але й активно освоювати нові перспективні сервіси, що дозволяють швидко і якісно їх надавати, зробити максимально простими і доступними для клієнтів. До того ж, якщо банк зацікавлений у залученні більшої кількості клієнтів та отриманні максимального прибутку, він повинен надати обслуговування в будь-який час та у будь-якому місці. Саме стратегії всебічної присутності та доступності відповідає дистанційне банківське обслуговування.

«***Дистанційне банківське обслуговування*** – це проведення операцій по рахунках клієнта на підставі його дистанційних розпоряджень, а дистанційне розпорядження – це розпорядження банку виконати певну операцію, передане клієнтом погодженим каналом доступу із певною процедурою передачі розпоряджень.» [5].

Отже, сутність дистанційного банківського обслуговування полягає у самообслуговуванні клієнтів. Технологія самообслуговування є технологічним видом взаємодії банку з клієнтами, яка дозволяє їм обслуговуватися незалежно від працівника банківського сервісу.

У теорії та практиці банківської справи поняття дистанційного (віддаленого) банківського обслуговування іноді розуміється як лише обслуговування клієнтів банків у мережі Інтернет, але, все ж таки, частіше – ототожнюється з каналами доставки, що не потребують втручання

банківського працівника, тобто між операційною системою та клієнтом немає посередників.

Головною метою використання засобів та прийомів дистанційного обслуговування в банківській діяльності є надання рівних можливостей оперування фінансовими інструментами в будь-яких регіонах країни та за її межами. Це забезпечує принципово новий рівень доступності банківського бізнесу при збереженні чи підвищенні його якості за рахунок створення мобільного інформаційного середовища та скорочення питомих витрат на одного клієнта, порівняно з традиційними системами обслуговування.

Дистанційна форма обслуговування клієнтів не залежить від відстані та часу, оскільки електронні канали працюють цілодобово та у будь-якій точці земної кулі, там, де є система телекомунікації. Для клієнта зникають поняття «операційний день», «технічна перерва», а головне – змінюється характер його взаємодії з банком. Для ефективнішого ведення діалогу з клієнтами сучасні банки почали розвивати сервіси дистанційного обслуговування, такі як «клієнт-банк», Інтернет-банкінг, відеобанкінг, телефонний банкінг (телебанкінг), мобільний банкінг, SMS-банкінг, мережі банкоматів (АТМ) та ін.

За допомогою таких видів дистанційного обслуговування клієнт має можливість здійснювати ті ж самі стандартні операції, що і у «фізичному» офісі банку (за винятком операцій з готівкою), а саме:

- здійснювати всі види комунальних платежів (за електроенергію, газ, тепло- та водопостачання, квартплату, телефон та ін.);

- оплачувати рахунки за зв’язок (стільниковий та пейджинговий зв’язок, Інтернет) та інші послуги (супутникове телебачення, навчання тощо);

- здійснювати грошові перекази у національній та іноземній валютах на будь-який рахунок у будь-якому банку;

- переказувати грошові кошти в оплату за товари, у тому числі куплені через Інтернет-магазини;

- купувати та продавати валюту;

- поповнювати та/або знімати грошові кошти з рахунку за допомогою платіжної картки;

- відкривати різні види рахунків та переказувати на них грошові кошти;

- одержувати інформацію про здійснені платежі в режимі реального часу;

- одержувати інші види послуг: брокерське обслуговування (купівля/продаж цінних паперів, створення інвестиційного портфеля), підписку на журнали, газети та ін.

Крім того, здійснення дистанційного банківського обслуговування мінімізує використання людської праці, сприяє скороченню організаційних витрат, зменшує деякі види ***банківських ризиків***, таких як втрата платіжних документів, їх фальсифікація, неправильна адресація, знижує ймовірність помилок у реквізитах платежу, прискорює обмін інформацією між банками та клієнтами, обробка платежів здійснюється переважно у реальному часі, зростає швидкість проходження платежів тощо [4, с. 43].

Спосіб дистанційного надання послуг клієнтам у сфері банківського обслуговування перетворився на цілком самостійну форму ведення бізнесу. Технологія дистанційного банківського обслуговування «домашній банкінг» (home banking), або «віддалений банкінг» (remote banking), що дає змогу клієнту отримувати банківські послуги, не відвідуючи офіс банку, існує вже більше двадцяти років.

Як видно із самої назви, «віддалений банкінг» – це у загальному випадку надання банківських послуг не в банківському офісі при безпосередньому контакті клієнта і банківського службовця, а в офісі клієнта, в його будинку і скрізь, де це допускається системою і зручно клієнту. Технологія «home banking» була розроблена на початку 80-х років,

коли банки Західної Європи розпочали активну конкуренцію за залучення нових клієнтів.

Впровадження системи «клієнт-банк», або комп'ютерного банкінгу (PC-banking) в Україні, стало однією з перших вдалих спроб українських банків з поліпшення обслуговування клієнтів та удосконалення власної роботи за допомогою автоматизованих систем. Спеціалісти стверджують, що таку систему вперше було використано в Україні у 1992 році. Беручи до уваги складні економічні умови того часу, а головне, практично відсутність розвинутого ринку комп'ютерної техніки, система «клієнт-банк стала своєрідним «проривом» у банківській справі. До речі, відсутність нормативно-правової бази для використання електронного цифрового підпису не стало тоді перешкодою на шляху широкого розповсюдження цієї послуги в нашій країні.

Система «клієнт-банк» являє собою програмно-технічний комплекс, який реалізує доступ клієнта до автоматизованої системи банку за допомогою персонального комп'ютера, здійснюваний за допомогою прямого з'єднання з банківською мережею з використанням модему. Наявність такої системи дає змогу клієнту, не виходячи з офісу, відправити до банку платіжне доручення, оперативно отримати інформацію щодо проходження платежу, стану поточного рахунку, а також документів, проведених за рахунком у будь-який момент часу.

Отже, основною функцією системи «клієнт-банк» є надання можливості клієнту – юридичній особі, наприклад підприємству, здійснювати платежі зі свого поточного рахунку в банку з власного офісу, не відвідуючи банківської установи.

Крім того, система «клієнт-банк» дозволяє користувачам керувати своїми рахунками в банку та одержувати поточну інформацію про рух коштів, а саме:

- проводити платежі зі свого рахунку в банку, не відвідуючи банк, з робочого місця в офісі, обладнаного персональним комп'ютером із встановленим необхідним програмним забезпеченням:

- відстежувати наявні грошові кошти на поточному рахунку та контролювати їх рух;

- отримувати виписки з поточного рахунку, а також дані щоденних офіційних курсів НБУ;

- вести довідник своїх контрагентів за платежами та довідник призначення платежу, що дозволяє швидше формувати платіжні документи. Зникає необхідність заносити інформацію до кожного документу – готовий шаблон переноситься до платіжного документу з довідників;

- робити архівні копії оброблених документів та переглядати документи з архіву;

- обмінюватися з банком нерегламентованими повідомленнями та завантажувати файли, передані банком, а також передавати власні файли;

- отримувати від обслуговуючого банку повідомлення про нові банківські послуги, поточні відсоткові ставки за кредитами та депозитами, а також іншу інформацію.

Клієнт також може звернутись до банку у будь-який момент часу, що забезпечує динамічність обміну інформацією між клієнтом та банком.

Загалом можна виділити такі переваги системи «клієнт-банк»:

1. Зручність. Забезпечує автоматизовану підготовку таких документів, як платіжне доручення, меморіальний ордер, заявка на переказ валюти та інших документів. Шаблони для введення електронних документів використовуються згідно з типовими стандартами, які діють в Україні і максимально наближені до паперових. Як і паперові, електронні платіжні документи, що відправлені до банку, підписують посадові особи підприємства, але замість звичайного, використовують електронний цифровий підпис.

2. Оперативність. При використанні системи «клієнт-банк» збільшується швидкість проходження платежів. Висока оперативність зумовлена тим, що платіжне доручення в електронному вигляді готується один раз, і це робить не операціоніст банку, а працівник підприємства. Крім того, не потрібно готувати первинні платіжні документи на паперових носіях. Замість них раз на тиждень готується реєстр електронних документів, внаслідок чого відпадає необхідність щоденно відвідувати банк для проведення безготівкових платежів, що, в свою чергу, економить час та гроші.

3. Мобільність. Система «клієнт-банк» дозволяє контактувати з банком без обмежень у часі, оскільки технічні можливості більшості програмних комплексів дозволяють цілодобово відправляти документи до банку та переглядати отримані звідти.

4. Безпека. Засоби захисту інформації в системі «клієнт-банк» при коректному їх використанні гарантують надійний захист від несанкціонованого доступу та модифікації інформації.

Отже необхідно зазначити, що система «клієнт-банк» не лише доволі зручна для клієнта при роботі з банком (для підприємств з великою кількістю філій та відділень у різних регіонах система дає можливість контролювати рух коштів в усій мережі), але й слугує відмінною платформою для прийняття оперативних рішень. Також система просто життєво необхідна тим підприємствам, що здійснюють велику кількість платежів протягом операційного дня.

Але поряд з очевидними перевагами, система «клієнт-банк» має і певні недоліки. Основним недоліком є те, що переказ коштів з використанням даної системи потребує постійної присутності керівних осіб – директора та головного бухгалтера, які наділені правом першого та другого підпису. Інакше керівники підприємства мусять відкрити електронний підпис іншим особам, що збільшує небезпеку несанкціонованого використання коштів на поточному рахунку. Крім

цього, можуть виникнути помилки при перенесенні інформації з системи «клієнт-банк» до автоматизованої банківської системи банку (АБС), якщо ці системи створювалися різними розробниками. Тож доречним було б визначити, наскільки сумісними є програмний комплекс «клієнт-банк» і АБС, що використовується в банку. Також висока ціна розробки і впровадження системи «клієнт-банк» робить її неефективною для невеликих банків, а необхідність завантаження й оплати спеціального програмного забезпечення обмежує коло потенційних клієнтів.

Система дистанційного банківського обслуговування (ДБО), за умови правильного використання, дозволяє збільшити безпеку і конфіденційність документообігу з банком; в будь-який момент отримати виписку, що містить інформацію про всі вхідні і вихідні документи в розширеному форматі, без відвідування банку. У той же час, системи ДБО, як інструмент доступу до грошових переказів, сьогодні все частіше стають мішенню для злочинців-шахраїв, яких також називають «кіберзлочинцями».

Втручання в роботу систем ДБО найчастіше відбувається шляхом зараження комп'ютера вірусним програмним забезпеченням через шкідливу спам-розсилку, відвідування заражених сайтів або використання заражених магнітних носіїв. Завантаження вірусу на комп'ютер жертви відбувається практично непомітно. Основне завдання вірусу на початковому етапі – це спостереження, збір інформації і передача його на комп'ютер шахраїв. Вірус може викрадати паролі доступу до систем ДБО, ключі електронного цифрового підпису, зчитувати реквізити платежів. Це також можуть бути програми, що відстежують появу на екрані вікна підключення до ДБО з метою подальшого перехоплення секретної інформації, яка вводиться в це вікно, або копіюють вміст буфера обміну в момент підключення до систем електронних платежів. Мета шахраїв спотворити інформацію, сформувати за допомогою ДБО і провести платіж, який за змістом не буде виділятися в потоці звичайної діяльності

жертви, але переведе гроші на рахунки підставної особи або фіктивної фірми, використовуючи звичайне для даного клієнта призначення платежу. В подальшому найчастіше кошти вкрадені з рахунку переводяться в готівку. Зняття готівки проводиться в основному через банкомати з метою уникнення спілкування з працівниками банку.

2. Кримінально-правова та криміналістична характеристика злочинів, вчинених шляхом несанкціонованого доступу до систем дистанційного банківського обслуговування

Несанкціонований доступ у діяльність системи дистанційного банківського обслуговування з метою злочинного збагачення являє собою комплекс (ланцюг) послідовних дій у структурі технології злочинного збагачення. Кримінально-правова кваліфікація дій зловмисників передбачена наступними статтями Кримінального кодексу України (КК України). Насамперед це статті: 185 КК України «Таємне викрадення чужого майна (крадіжка)»; ст. 190 КК України «Шахрайство» (у якій також зазначено, що шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки); ст. 200 КК України «Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей»; ст. 231 КК України передбачає відповідальність за умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких

відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності; ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації».

Хотілося б детальніше зупинитися на розгляді ст. 361 КК України. У цій статті передбачено відповідальність за несанкціоноване втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підроблення, блокування інформації, спотворення процесу автоматичної обробки інформації або до порушення встановленого порядку її маршрутизації.

Об'єктом такого злочину є ЕОМ, АС, комп'ютерні мережі та мережі електрозв'язку. Об'єктом такого злочину також може бути право власності на комп'ютерну інформацію. У роз'ясненні Верховного Суду України щодо узагальнених матеріалів слідчо-судової практики розгляду справ за ст. 361 КК України вказано: «для визнання факту вчинення злочину, склад якого передбачено у ст. 361 КК, слід встановити не лише вчинення діяння, а й настання хоча б одного із зазначених в законі наслідків: витоку, втрати, підроблення, блокування інформації, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації. Тобто між несанкціонованим втручанням в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку має бути причинний зв'язок хоча б з одним із суспільно небезпечних наслідків» [6].

Специфіка розгляду справ цієї категорії полягає у правильному розумінні термінів, визначення яких містяться у наведених вище нормативних документах.

ЕОМ розуміється як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної

обробки інформації при вирішенні обчислювальних та інформаційних завдань.

АС – це організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв'язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп'ютера, то АС — це й окремо взятий комп'ютер разом з його програмним забезпеченням.

Комп'ютерна мережа — це сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається у системі іншої ЕОМ.

Мережа електрозв'язку — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Об'єктивна сторона злочину проявляється у формі несанкціонованого втручання в роботу ЕОМ, їх систем, комп'ютерних мереж чи мереж електрозв'язку, наслідком якого є: 1) витік; 2) втрата; 3) підроблення; 4) блокування інформації; 5) спотворення процесу автоматичної обробки інформації; 6) порушення встановленого порядку її маршрутизації.

Несанкціоноване втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж — це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машин, їх систем чи комп'ютерних мереж або повністю чи частково припиняють їх роботу без дозволу відповідного власника або уповноваженої особи.

Несанкціонованим втручанням в роботу мереж електрозв'язку слід вважати будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж, що забезпечують роботу мереж електрозв'язку) вчинені без згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких припиняється (зупиняється) робота мережі електрозв'язку або відбуваються зміни режиму цієї роботи.

Комп'ютерна інформація — це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може бути створена, змінена чи використана за допомогою ЕОМ [6].

Предметом злочину є: 1) інформація, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку; 2) технічні засоби автоматизованої обробки та захисту інформації (елементи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку).

Як *предмет* злочину, інформація, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, має притаманні ознаки фізичного, економічного та юридичного характеру.

Інформація матеріалізується в носіях інформації, якими можуть бути фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах. Носіями інформації в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку виступають тверді фізичні об'єкти (жорсткі диски, дискети, компакт-диски тощо), сигнали (у каналах зв'язку), поля (оперативна пам'ять ЕОМ та її периферійних пристроїв). Носії інформації можуть бути вилучені з володіння законного власника або пошкоджені чи знищені. Інформація, яка оброблюється в електронно-обчислювальних машинах

(комп'ютерах), автоматизованих системах та комп'ютерних мережах, зберігається на носіях такої інформації у формі даних.

Правова охорона інформації, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах та комп'ютерних мережах або пересилається каналами електрозв'язку, зумовлена не статусом цієї інформації як об'єкта власності, а її змістом, споживчою цінністю, здатністю задовольняти інформаційні потреби.

Інформація є чужою для винного (не перебуває у власності чи законному володінні винного), належить на праві власності іншому суб'єкту власності. Суб'єкти права власності на інформацію визначаються авторським правом або договірними відносинами. Власник інформації, уповноважені ним на те особи визначають користувачів належної йому інформації та встановлюють їх повноваження.

Сукупність усіх даних і програм являє собою інформацію, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах та передаються мережами електрозв'язку незалежно від засобу їх фізичного та логічного представлення.

Обов'язковою ознакою об'єктивної сторони є *несанкціонованість* втручання. Санкціонованим вважається втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку з дозволу власника, а також уповноважених власником осіб або службових осіб на яких покладено забезпечення їх нормальної роботи.

Для правомірного отриманням необхідних інформаційних продуктів та їх використання користувач інформації повинен звертатися за дозволом до власника інформації, її володаря або розпорядника.

Як правило захист інформації (запобігання вільному доступу до інформації, усунення технічних каналів її витоку тощо) в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах та

мережах електрозв'язку забезпечується комплексом організаційних, програмних і технічних заходів.

Несанкціонований доступ може бути здійсненим *двома способами*:

- безпосереднє проникнення в заборонену зону, приміщення де оброблюється інформація з подоланням програмних, технічних чи організаційних заходів;

- опосередковано - віддалений доступ з використанням програмних та технічних засобів для подолання захисту.

Злочин вважається закінченим з моменту настання одного або декількох із зазначених у статті наслідків: 1) виток інформації; 2) втрата інформації; 3) підробка інформації; 4) блокування інформації; 5) спотворення процесу обробки інформації; 6) порушення встановленого порядку маршрутизації інформації.

Злочинна акція, направлена на несанкціонований доступ до мережі даних банківської установи також може закінчуватись знищенням електронно-обчислюваної техніки (пристроїв), яка була використані для здійснення злочину. Мета – знищення слідів злочину. Фізичне знищення або пошкодження ЕОМ (комп'ютерів), інших технічних засобів автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, якщо умисел винного було спрямовано саме на це, кваліфікується за ст. 194 КК України ("Умисне знищення або пошкодження майна ").

Факт перегляду інформації за результатом несанкціонованого доступу можна кваліфікувати за ст. 361 у разі настання наслідку ─ витоку інформації з обмеженим доступом. Одержання несанкціонованого доступу правопорушником, у більшості випадків, блокує інформацію (або інформаційну послугу) призначену для законного користувача (наприклад, несанкціонований доступ до мережі Інтернет з використанням чужих паролів). В інших випадках, коли дії особи хоч і пов'язані з несанкціонованим доступом, але не спричинили суспільно-небезпечних наслідків, це можна кваліфікувати, в залежності від обставин, як

готування до вчинення іншого умисного злочину ─ усунення перешкод, інше умисне створення умов для вчинення злочину (ст. 14 КК України) або замах на злочин ─ якщо злочин не було доведено до кінця з причин, що не залежали від її волі (ст. 15 КК України).

У випадку коли несанкціоноване втручання виступає способом вчинення іншого умисного злочину, а технічні засоби використовуються в якості знаряддя для досягнення злочинної мети, вчинене винним кваліфікується по сукупності злочинів.

Суб'єкт злочину, передбаченого статтею 361 КК України ─ загальний. Це фізична особа, яка не має права доступу до певної інформації, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку або до технічних засобів її автоматизованої обробки.

Якщо особа має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, то її дії кваліфікуються за ст. 362 ("Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї") або ст. 363 ("Порушення, правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється ") КК України.

Суб'єктивна сторона злочину характеризується умисною формою вини. Злочинні дії при подоланні програмного та технічного захисту для отримання несанкціонованого доступу можуть бути вчинені лише з прямим умислом, тоді як ставлення винного до наслідків несанкціонованих дій з ЕОМ (комп'ютерами) може характеризуватись як прямим так і непрямим умислом.

Особа, яка здатна втрутитись у роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку має відповідні знання, вміння та навички автоматизованого оброблення інформації. Винна особа:

- усвідомлює соціальну небезпечність несанкціонованого втручання, його протиправність;

- передбачає наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворенню процесу обробки інформації або до порушення встановленого порядку її маршрутизації;

- бажає або свідомо припускає настання цих наслідків, ставиться до їх настання байдуже.

Мотив переважно корисливий, але можливі - помста, хуліганство, підрив репутації, приховування іншого злочину тощо.

Повторністю злочинів визнається вчинення двох або більше злочинів, передбачених цією статтею або її частиною (ч.1 ст.32 КК України). Повторність підвищує суспільну небезпечність вчиненого, а тому враховується як обтяжуюча обставина при призначенні покарання (п.1 ст.67 КК України).

Поняття *"вчинення злочину за попередньою змовою групою осіб"* надається в ч. 2 ст. 28 КК України. Злочин вважається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку злочину, домовились про спільне його вчинення.

Вчинення злочину за попередньою змовою групою осіб може мати місце в наступних випадках:

– несанкціоноване втручання вчиняється двома або більше співучасниками, кожен з яких виконує всі дії, що утворюють об'єктивну сторону цього складу (наприклад, декілька злочинців здійснюють незаконне втручання з окремих терміналів і знищують певну інформацію);

– несанкціоноване втручання вчиняється двома або більше співучасниками, кожен з яких виконує частину дій, що характеризують об'єктивну сторону цього складу (наприклад, одна особа вчиняє несанкціоноване втручання, а друга – знищує інформацію про таке втручання);

– несанкціоноване втручання вчиняється двома або більше особами, при цьому лише одна з осіб виконує роль виконавця, а інші є підбурювачами, пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє незаконне втручання, що призводить до спотворення процесу обробки інформації).

Вимоги до співучасників, передбачені ст.26 КК України є обов'язковими у всіх випадках.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, відноситься до злочинів з матеріальним складом, а тому настання наслідків є обов'язковою ознакою.

Відповідно до ч.2 ст.11 КК України не є злочином будь-яка дія навіть якщо формально вона і містить ознаки злочину, але не становить суспільної небезпеки через малозначимість, тобто не заподіяла і не може заподіяти істотної шкоди.

Криміналістична характеристика. Розглянувши кримінально-правову характеристику цих злочинів, хотілося б відмітити, що ми їх об'єднуємо у криміналістично однорідну групу під умовною назвою «Технологія злочинної діяльності за допомогою несанкціонованого втручання у діяльність ДБО». Ця технологія складається із розглянутих злочинів, які є певними етапами у ланцюгу злочинної поведінки, кінцевою метою яких є – протиправне збагачення. Останнє може кваліфікуватися або ж за ст. 185, 190 КК України, або ж за ст. 191 КК України у випадку, якщо зловмисник(и) є посадовою особою з відповідними повноваженнями. Тобто злочинні посягання у сфері ДБО мають місце у наступних випадках:

1) коли до вчинення злочинів причетні представники банківського сектору з використанням наданих їм повноважень щодо доступу до фінансових ресурсів відповідної фінансової установи (внутрішнє втручання);

2) коли злочинні посягання на ресурси банку здійснюються особами, які не мають відношення до банківської установи (зовнішнє втручання).

3) змова осіб першої та другої групи (організована група осіб).

Для механізму вчинення злочинів шляхом несанкціонованого втручання у діяльність ДБО організованими злочинними групами є характерним розподілення функцій між окремими її членами, коли кожний з них виконує тільки частку злочинної «роботи», яка підлягає кваліфікації за окремою статтею Кримінального кодексу України (далі КК України). Завдання правоохоронних органів у таких ситуаціях полягає у тому, щоб за окремими ланцюжками злочинних дій окремих осіб розгледіти єдину злочинну діяльність організованої групи. Характеризується це наявністю *основних* і *допоміжних* злочинів. Вони відображають логіку поведінки злочинців і є певними етапами в досягненні злочинної мети. *Допоміжні* злочини можуть виступати необхідною передумовою скоєння інших, або виступають формою, способом здійснення основного злочину. *Мета основного* злочину полягає в отриманні певної матеріальної вигоди і знаходиться в основі мотивації злочинної поведінки суб'єкта, як було розглянуто вище. Таким чином уся злочинна діяльність набуває вигляду складних взаємопов'язаних діянь, суттєвість якої адекватно відображує термін технологія злочинної діяльності.

Аналіз практики вказує, що при досудовому розслідуванні цієї категорії кримінальних справ мають місце труднощі у доказуванні злочинних дій, що викликані складними, заплутаними схемами злочинних технологій. Як вже зазначалося, при розслідуванні організованої злочинної діяльності важливо довести наявність необхідного зв'язку між окремими діями (злочинами), що складають загальну «картину» технології

злочинного збагачення. А це, як вказує слідчо-судова практика зробити досить важко. Тому слід враховувати закономірності, пов'язані зі скоєнням та розслідуванням кількох злочинів. Розглянемо детальніше зміст технологій злочинного збагачення за допомогою несанкціонованого втручання у діяльність ДБО.

Останнім часом активність кіберзлочинців значно зросла щодо втручання в ДБО, зокрема системи «Клієнт-Банк». Причому зменшується вплив одиночок і збільшується – організованих груп злочинців. Якщо ще два роки тому це були поодинокі випадки, то в 2013-2014 рр. кількість і обсяг злодійських трансакцій зросли в рази. Банкіри також занепокоєні тим, що у 2013 р. зафіксовані випадки масового застосування проти банків (одночасно проти десяти і більше банків) розподілених кібератак на зовнішні сервіси типу «відмова в обслуговуванні» (DDos-атаки) [5].

Несанкціонований доступ до систем ДБО в більшості випадків шахраї отримують з вини клієнтів. Шахраї виводять досить великі суми з рахунків юридичних осіб, після чого переводять їх по ланцюжку з фіктивних юридичних або фізичних осіб і знімають готівкою. По рахунках фізичних осіб шахрайство в системах ДБО незначне. Як вказує практика, більшість крадіжок відбуваються наприкінці тижня, після 17:00 у п'ятницю, а власники рахунків дізнаються про це лише в понеділок, коли шахрайська операція давно завершена і гроші перекочували через десяток рахунків.

За даними МВС, в 2012 р. правоохоронними органами встановлено 129 фактів втручання в роботу систем ДБО з метою крадіжки коштів. У результаті цих операцій з рахунків юридичних осіб - клієнтів банків «списано» 116 млн. грн, 75% з яких органи МВС змогли повернути власникам або заблокували за результатами слідчих дій [4].

Технологія злочинного збагачення шляхом несанкціонованого втручання в діяльність ДБО складається з наступних найбільш типових схем по підготовці, здійсненню та приховані слідів злочинів:

1. Розповсюдження комп'ютерних вірусів для отримання реквізитів персональних комп`ютерів при розрахунках в мережі Інтернет, що дає можливість для отримання паролів, логінів та ключів користувачів систем дистанційного банківського обслуговування.

2. Шахрайство з використанням дистанційного банківського обслуговування (система «клієнт-банк», тощо).

3. Використання пристроїв для незаконного отримання даних ПК та ПІН-коду до неї (Скіммінг).

4. Отримання персональних даних держателів платіжних каток (номер карти, PIN- або CVV/CVC код) з наступним використанням цих даних для виготовлення копій платіжних карток (Так званий «Кардінг» - отримання персональних даних держателів платіжних каток (номер карти, PIN- або CVV/CVC код).

5. Викрадення особистої інформації (наприклад, реквізитів банківських рахунків, паролів доступу).

Це може здійснюватися шляхом так званих *«фішингу»* або *«вішингу»*. Фішинг – намагання витягнути з власника картки інформацію, наприклад, шляхом направлення листа електронною поштою із посиланням на Інтернет-сайт де необхідно вказати свої персональні дані. Створення шахраями «клонів» сайтів відомих банків, Інтернет - магазинів і т.п., на яких держателі вводять реквізити спеціальних платіжних засобів. Вішинг – коли використовується технологія передачі мовного сигналу через мережі Інтернет. Наприклад - дзвінок від представника банку або автоматичного інформатора про заблокування рахунку електронного зв’язку.

Попри це, банками запроваджуються додаткові механізми захисту рахунків клієнтів від несанкціонованого втручання у ДБО, а саме:

- по клієнтської програмі клієнт-банк-OnLine - перед відправкою документів на проведення, клієнтом вводиться комбінація «картинок» або таємного коду, отриманого на свій мобільний телефон у вигляді sms-

повідомлення;

- вводяться технологічні процедури запобіганню шахрайства при проведенні операцій з платіжними картками, а саме: 100-відсоткова авторизація всіх операцій в торгово-сервісній мережі; примусове введення на терміналі останніх 4 ембосованих цифр номера картки при формуванні запиту і зіставлення їх з даними на магнітній смузі. У разі якщо дані не співпали, операція не дозволяється;

- вводяться лімітування на максимальну суму покупки, на максимальну кількість операцій, максимальну суму операцій за однією карткою і т.д.;

- запроваджується підтвердження правомірності надходження платіжних документів клієнта, отриманих за допомогою системи «клієнт-банк», на значні суми, а також тих, що є нетиповими для клієнта, в телефонному режимі у відповідальних осіб;

- банк, за погодженням з клієнтом, здійснює контроль відповідності електронного цифрового ключа з IP – адресою робочої станції клієнта, на якій встановлено Інтернет – банкінг та здійснюється відправка платежів (при наявності статичної IP – адреси);

- виявлення несанкціонованих клієнтами перерахунків коштів через систему «клієнт-банк» створена група розсилки «anti-fraud» в яку входять співробітники підрозділів, що приймають участь в попередженні та розслідуванні таких випадків. На дану групу направляються повідомлення щодо підозр та фактів шахрайства, як безпосередньо від співробітників Банку, так і в автоматичному режимі при фіксуванні підключень з IP-адрес, комп'ютерів, з яких раніше фіксувались випадки та спроби шахрайства, та автоматичні повідомлення про формування платіжних документів на контрагентів, на яких вже були зафіксовані несанкціоновані платежі та їх спроби.

Неправомірний (або несанкціонований) доступ до автоматизованих інформаційних систем (АІС) або мереж – є небезпечним, дуже латентним і

розповсюдженим видом злочинів у сфері високих технологій. Як вже зазначалося, несанкціонований доступ часто стає першочерговим етапом вчинення інших видів злочинів у технології злочинного збагачення шляхом несанкціонованого втручання у мережу ДБО.

При проведенні кримінального провадження, пов'язаного із незаконним доступом до комп'ютерної інформації може бути визначено декілька місць вчинення одного злочину, а саме:

а) місця безпосередньої обробки та зберігання інформації;

б) місця безпосереднього використання технічних засобів для неправомірного доступу до комп'ютерної інформації;

в) місця зберігання інформації на машинних носіях;

г) місця безпосереднього використання результатів неправомірного доступу до комп'ютерної інформації.

Час вчинення злочину: частіше всього такі злочини вчинюються в період роботи комп'ютерів і не обмежуються певним відрізком часу, оскільки АІС можуть функціонувати цілодобово.

2.1. Способи вчинення злочинів

Способи вчинення злочинів у схемах збагачення за допомогою сфери ДБО можливо класифікувати за методами перехоплення інформації, методами доступу до баз даних та методи маніпуляцій.

1. Методи перехоплення.

1.1. ***Безпосереднє перехоплення*** – найдавніший з використовуваних способів. Необхідне устаткування можливо придбати в магазинах: мікрофон, радіоприймач, касетний диктофон, модем, принтер. Перехоплення інформації здійснюється безпосередньо через телефонний канал системи, або підключенням до комп'ютерних мереж. Вся інформація записується. Об'єктами прослуховування являються різні системи – кабельні і дротяні, наземні мікрохвильові, супутникового і урядового

зв'язку.

1.2. ***Електромагнітне перехоплення.*** Використовуються перехоплюючи пристрої, які працюють без прямого контакту. Можливо вловити випромінювання центральним процесором, дисплеєм, телефоном, принтером, прочитувати дані з дисплейних терміналів за допомогою доступних кожному найпростіших технічних засобів (додаткової антени, телевізора). Злочинці, знаходячись в автомобілі або просто з приймачем у портфелі на відстані від будівлі, можуть не привертаючи до себе уваги, легко дізнатися про данні, які зберігаються в пам'яті ЕОМ або використовуються в процесі роботи.

1.3. ***Використання "жучків"*** полягає в установці мікрофону в комп'ютері з метою прослуховування розмов персоналу. Цей прийом, зазвичай який використовується як допоміжний для отримання інформації про роботу комп'ютерної системи, про персонал, про заходи безпеки і т.д.

1.4. ***"Прибирання сміття"*** – пошук даних, залишених користувачем після роботи з комп'ютером. Включає **фізичний** варіант – огляд вмісту корзин для сміття та збір залишених за непотрібністю роздруківок, ділового листування та інше. **Електронний** варіант заснований на тому, що останні з збережених даних зазвичай не знищуються після закінчення. Інший користувач записує тільки невелику кількість своєї інформації, а потім спокійно зчитує попередні записи і збирає потрібну йому інформацію таким чином можуть бути виявлені паролі, приз віща користувачів та інше.

2.Методи несанкціонованого доступу.

2.1. ***"За дурнем"*** – використовується для входу в закриті для доступу приміщення або термінали. **Фізичний** варіант полягає в тому, що взявши в руки якомога більше предметів, пов'язаних з роботою на комп'ютері, проходжується з діловим виглядом біля зачинених дверей, за якими знаходиться термінал, і, коли з'явиться законний користувач, впевнено пройти з ним у двері. Електронний варіант проходить, коли комп'ютерний

термінал незаконного користувача підключається до лінії законного через телефонні канали (Інтернет) або користувач виходить ненадовго, залишаючи термінал в активному режимі.

2.2. ***Комп'ютерний абордаж*** - хакери, набираючи навмання один номер за іншим, очікують доки на іншому кінці дроту не відкликнеться чужий комп'ютер. Після цього телефон підключається до приймача сигналів у власній ЕОМ, і зв'язок встановлено. Залишається вгадати код (а слова, які служать паролем, частіше банальні та беруться з інструкції про користування комп'ютером) і стає можливим втрутитися в чужу комп'ютерну систему.

2.3. ***Поступовий вибір*** – несанкціонований доступ до файлів законного користувача через слабкі місця у захисті системи. Одного разу виявивши їх, порушник може не поспішаючи дослідити інформацію, що міститься в системі, копіювати її повертатися до неї багато разів.

2.4. ***"Маскарад або самозванство***" – дехто проникає в комп'ютерну систему, видаючи себе за законного користувача. Системи, які не володіють засобами автентичної ідентифікації (наприклад, за фізіологічними характеристиками: по відбиткам пальців, по малюнку сітківки ока, голосу та інше), виявляються без захисту проти цього прийому. Найпростіший шлях його здійснення – отримати коди та інші ідентифікуючі шифри законних користувачів.

2.5. ***Містифікація*** - користувач з знищеного термінала випадково підключається до чиєїсь системи, будучи абсолютно впевненим, що він працює з тією системою, з якою і намагався. Володар цієї системи формує правдоподібні відклики, якийсь час підтримує цю помилку, отримує одночасно деяку інформацію, зокрема коди.

2.6. ***"Аварійний"*** - використовується той факт, що в любому комп'ютерному центрі є особлива програма, якою користуються в разі виникнення порушення або інших відхилень в роботі ЕОМ.

2.7. ***"Склад без стін"*** - несанкціонований доступ здійснюється в разі

системної поломки. Наприклад, якщо деякі файли у користувача залишаються відкритими, він може отримати доступ до файлів які йому не належать.

3. Методи маніпуляції.

3.1. ***Підміна даних*** **–** зміни, або введення даних здійснюється, як правило, при вводі або виводі інформації з ЕОМ.

3.2. ***Маніпуляції з пультом управління*** **–** механічна дія на технічні засоби машини створює можливості маніпуляції даними.

3.3. ***”Троянській кінь”*** – таємне введення в чужу програму команд, які дозволяють, не змінюючи працездатність програми, здійснити визначені функції. Цим способом злочинці зазвичай відраховують на свій рахунок певну частку з кожної операції. Одним із варіантів є ”Салямі”, коли відраховані суми малі і їх втрати практично непомітні (наприклад, по 1 долару з операції), а накопичення здійснюються за рахунок великої кількості операцій. Це один з найпростіших і безпечних способів, особливо якщо відраховуються невеликі дробові суми, оскільки в цих випадках зазвичай все одно робиться округлення.

3.4. ***”Бомба”*** – таємне вбудовування в програму набору команд, які повинні спрацювати (або кожний раз спрацьовувати) при певних умовах або в певний момент часу.

3.5. ***Моделювання*** процесів в які злочинці бажають втрутитися, і планування методів вчинення і приховування посягань для оптимізації способу злочину. Одним із варіантів являється реверсивна модель конкретної системи в яку вводяться реальні початкові данні і враховуються дії які плануються. Із отриманих результатів підбираються правдоподібні. Потім, шляхом прогону моделі назад, до початку, з’ясовують результати і встановлюють, які маніпуляції з початковими даними необхідно проводити. Таких операцій може бути кілька. Після цього залишається тільки здійснити задумане.

3.6. ***”Повітряний змій”*** – спосіб, який досить часто

використовується. В двох банках (але можливо і в кількох) відкривають невеликій рахунок і переводять гроші з одного банку в інший і навпаки з сумами, що поступово підвищуються. Хитрість полягає в тому, що до моменту, коли в банку виявиться, що доручення про переказ не забезпечено відповідною сумою, приходило б повідомлення про переказ в цей банк так, щоб загальна сума покривала вимогу про перший переказ. Цикл повторюється кілька разів до тих пір, доки на рахунку не виявиться достатня сума. Тоді гроші швидко знімаються і власник рахунку зникає. На практиці в таку гру включають велику кількість банків: так сума накопичується скоріше і кількість доручень про переказ не викликає підозри.

Встановлення *місця* несанкціонованого доступу до ДБО викликає певні труднощі, бо таких місць може бути декілька. Наприклад, при встановленні факту неправомірного доступу до інформації в локальній комп'ютерній системі чи мережі слід виявити місця, де розміщені комп'ютери, що мають єдиний телекомунікаційний зв'язок.

Простіше це завдання вирішується у разі несанкціонованого доступу до окремих комп'ютерів, що знаходяться в одному приміщенні. Однак, при цьому необхідно враховувати, що інформація на машинних носіях може знаходитися в іншому приміщенні, яке теж слід встановлювати.

Складніше встановити місце безпосереднього застосування технічних засобів несанкціонованого доступу, який був здійснений за межами організації, через систему глобальної електронної телекомунікації, наприклад, Internet. Для встановлення такого місця необхідно залучати фахівців, які мають спеціальні прилади та комп'ютерні програмні засоби виявлення несанкціонованого доступу. Встановленню підлягає також місце зберігання інформації на машинних носіях або роздруківок, отриманих у результаті неправомірного доступу до комп'ютерної системи чи мережі.

За допомогою комп'ютерних програм загальносистемного

призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволяє за відповідною командою вивести на екран дисплея інформацію про день, години, хвилини та секунди виконання тієї або іншої операції. При вході до системи чи мережі (в тому числі й несанкціонованому) час роботи на комп'ютері будь-якого користувача та час виконання конкретної операції автоматично фіксуються в оперативній пам'яті та відображаються, як правило, у вихідних даних на дисплеї, вінчестері та інших машинних носіях.

З урахуванням цього, час несанкціонованого доступу можна встановити шляхом огляду комп'ютера, роздруківок чи машинних носіїв інформації. Його доцільно виконувати за участю фахівця в галузі комп'ютерної техніки та технологій – програміста-математика, інженера-електронника. Необережне поводження або дії недосвідченої особи можуть випадково знищити інформацію, яка знаходиться в оперативній пам'яті комп'ютера або на носіях інформації.

Час неправомірного доступу до комп'ютерної системи можна встановити також шляхом опитування свідків з числа співробітників організації, де було встановлено цей факт. При цьому слід з'ясувати, коли саме кожен з них працював на комп'ютері, якщо це не було зафіксовано автоматично або в журналі обліку роботи на комп'ютері.

Як відомо, несанкціонований доступ до мереж ДБО є певним етапом по підготовці та здійсненню розкрадань грошових коштів клієнтів банку. Наступним етапом є переказ безготівкових коштів на рахунки фіктивних фірм чи окремих фізичних осіб, з наступною конвертацією грошей. Особливого значення у зв'язку з цим набуває розслідування обставин переводу одержаних безготівкових коштів у готівку (в тому числі в іноземну валюту). Розроблені та застосовані у кожному конкретному випадку схеми конвертації (переводу у готівку) коштів безпосередньо залежать від рівня організованості групи та попереднього підготування злочинів. І тут не виключена участь представників банківської установи.

Основною ознакою незаконної діяльності з конвертації та наступної легалізації злочинних доходів є створення *фіктивних фірм* (ст. 205 КК України). У диспозиції ст. 205 КК України вказано: «Фіктивне підприємництво - тобто створення або придбання суб'єктів підприємницької діяльності (юридичних осіб) з метою прикриття незаконної діяльності або здійснення видів діяльності, щодо яких є заборона». З *об'єктивної сторони* злочин може виявлятись у двох випадках: створенні юридичних осіб (суб'єктів підприємницької діяльності) або їх придбанні.

При здійсненні вищевказаних дій особа насправді не має на меті займатись підприємницькою діяльністю, передбаченою статутними документами, а бажає прикривати незаконну діяльність або здійснювати заборонену діяльність.

Некваліфікований склад злочину «фіктивне підприємництво» (ч. 1 ст. 205 КК) є формальним, тобто вважається закінченим з моменту створення або придбання фіктивного підприємства, установи чи організації.

Суб'єктивна сторона злочину характеризується прямим умислом. Це означає, що особа усвідомлює, що створює фіктивне підприємство, і бажає вчинити ці дії. Слід вказати, що мета є обов'язковою ознакою складу вказаного злочину. Вона може виявлятись у бажанні:

а) прикривати за допомогою створеної підприємницької структури незаконну діяльність (ухилення від сплати податків, порушення порядку заняття господарською та банківською діяльністю, легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом тощо);

б) займатись забороненими видами діяльності (діяльність, яка підлягає ліцензуванню, без ліцензії; діяльність, якою взагалі заборонено займатись підприємницьким структурам і т.п.).

Згідно п. 20 Постанови Пленуму Верховного Суду України «Про

практику застосування судами законодавства України про відповідальність за окремі злочини у сфері господарської діяльності» від 25 квітня 2003 року № 3, треба мати на увазі, що у разі, коли створений чи придбаний суб'єкт підприємницької діяльності розпочав незаконну діяльність, що містить ознаки ще й іншого злочину, дії винної особи належить кваліфікувати за сукупністю злочинів - за ст. 205 КК і тією статтею КК, якою передбачено відповідальність за здійснення незаконної діяльності.

Вивчення досвіду розслідування економічних злочинів у ряді регіонів України показує, що технологія злочинного збагачення з використанням статусу фіктивних суб'єктів підприємницької діяльності має форму організаційних і господарських дій засновників або керівників комерційних структур. Ці, зовні законні дії спрямовані, з одного боку, на утворення сприятливих умов для вчинення конвертації та легалізації незаконно отриманих доходів, а з іншого боку - на маскування злочинної діяльності з метою ухилення її організаторів від відповідальності. Будучи включеним у механізм здійснення економічних злочинів, фіктивне підприємництво істотно впливає на методику виявлення і розслідування цих злочинів.

Участь банківських працівників у ланцюгу злочинного збагачення шляхом незаконного доступу до мереж ДБО полягає у таких діях:

► забезпечення інформацією щодо рахунків клієнтів банку, наявність коштів, персональні дані, тощо;

► створення рахунків фіктивних фірм, або вигаданих фізичних осіб для перерахування грошей і купівлі іноземної валюти;

► переведення безготівкових коштів в готівку з використанням фіктивних фірм. Використовують такі фінансові інструменти: рахунки фізичних осіб, лоро-рахунки, систему електронних розрахунків, вексельну форму розрахунків тощо.

Механізм злочинної діяльності конвертаційних центрів забезпечується завдяки наступним безпосереднім діям працівників банку:

а) пошук та складання угоди з іноземним банком про відкриття кореспондентських рахунків;

б) відкриття поточних рахунків для фіктивного підприємства;

в) отримання індивідуальних валютних ліцензій;

г) забезпечення прикриття незаконних фінансових операцій за рахунками фіктивних фірм. Для цього використовують: внутрибанківські рахунки (на приклад, «Кошти до запитання», «Інші кредитори та дебітори»); канали зв'язку, що виключають факт здійснення переводу грошей через Національний банк і та ін.;

д) відкриття запасних рахунків (поточних, дебетових, кредитових) фізичних осіб за підробленими документами;

е) організація домовленостей з посадовими особами з контролюючих органів (наприклад, НБУ) .

Далі провідна роль керівників банків у цій системі зводиться до безперебійного постачання фірм конвертаційного центру та його клієнтів готівковою грошовою масою, забезпечення захисту безготівкових грошових коштів на рахунках фіктивних фірм від раптового блокування з боку правоохоронних та наглядових органів. У цьому випадку банківській сфері допомагає існування інституту банківської таємниці. Також зберігати «таємницю» злочинної діяльності комерційним банкам дозволяє те, що вони є суб'єктами первинного фінансового моніторингу. Фактично, на банк покладено основні контрольні функції з перевірки пакету наданих підприємством та завірених реєстраційних документів для відкриття рахунків; перевірки наданих документів, що підтверджують здійснення зовнішньоекономічної діяльності (контракти, вантажно-митні декларації та інше). Тому злочинна змова керівників банківських установ з бізнес-структурами для здійснення технології злочинного збагачення у цьому напрямку може довгий час залишатися непоміченою правоохоронними органами.

За таких умов керівники банків часто самі виступають ініціаторами

створення конвертаційних центрів та мережи фіктивних фірм з метою проведення несанкціонованого доступу до рахунків клієнтів та незаконних операцій з легалізації грошових коштів і приховання слідів від такої злочинної діяльності.

2.2. Характеристика особи злочинця та злочинних груп

Результати кожної злочинної діяльності містять сліди особи злочинця, що її здійснила, і, зокрема, інформація про його особисті соціально-психологічні властивості та якості, злочинний досвід, спеціальні знання, стать, вік, взаємодію з соціальними та індивідуальними життєвими умовами, які в тій чи іншій мірі вплинули на скоєння злочину. Відомості про особу, яка вчинила злочин, є одним із найважливіших структурних елементів криміналістичної характеристики. Говорячи про економічну злочинність у сфері банківського обслуговування клієнтів, хотілося б відмітити, що на даний час вона отримала якісно новий, професійно організований рівень. При розслідуванні групових злочинів цього напрямку не завжди враховуються всі специфічні риси сучасних організованих груп та характер їх діяльності. Тому встановлення причетності осіб до вчинення злочинів та притягнення їх до відповідальності залишається ключовою проблемою. Для прикладу, за даними МВС України уникнути відповідальності за скоєні злочини у сфері господарської діяльності вдається чи не кожному п’ятому з числа винних.

Вирішальною ознакою при встановлені суб’єктного складу економічних злочинів у сфері банківської діяльності є їх, певною мірою, відношення до цієї сфери. Це, насамперед, особи, які: 1) займають відповідні посади в установах банків; 2) посадові особи підприємств, установ та організацій різних форм власності, які своїми злочинними діями порушують охоронювані державою інтереси здійснення банківської

діяльності; 3) фізичні особи, які мають корисливу зацікавленість у здійсненні злочинів вказаного напрямку. Особливу увагу при розгляді злочинної діяльності щодо несанкціонованого доступу до систем та мереж ДБО заслуговують так звані кіберзлочинці. Тобто особи, які мають спеціальні знання та досвід щодо роботи і обслуговування ЕОМ.

Отже, механізм вчинення окремих злочинів вказаного виду обумовлюється об'єктивною можливістю здійснення певних дій з коштами, які знаходяться на рахунках банків, або з їх еквівалентами. Ця можливість, у свою чергу, залежить від службового становища конкретної особи, обсягу і характеру її повноважень, досвіду, злочинних зв'язків тощо.

Характеризуючи вказані групи осіб необхідно відмітити їх основні відзнаки. Більшості з них властиві порівняно високий рівень освіченості, прагнення до накопичення багатства будь-яким шляхом, швидка адаптація до змін нормативно-правового характеру, наявність широкого кола ділових стосунків та ін. Здійснення злочинів у цій сфері вимагає від учасників певних знань, навиків і спеціальної підготовки. Одній особі достатньо складно вирішити весь комплекс виникаючих проблем, тому нерідко на етапі підготовки до скоєння злочину та на етапі його реалізації діють абсолютно різні особи у складі злочинних груп. Корисливим злочинним діям осіб, головним чином, сприяють з одного боку умови слабкого контролю за порядком діяльності банків, а з іншого – можливість прикриття зловживань завдяки існуванню інституту банківської таємниці. Тому злочинці вміло використовують вже об'єктивно сформовані для них сприятливі умови вчинення злочинів.

Аналіз статистичних даних дозволяє зробити висновок про те, що протягом періоду з 1996 – 2012 рр. спостерігалася тенденція до збільшення реєстрації виявлених осіб, які вчинили злочини у банківській сфері, при загальному зниженні реєстрації працівників банківських установ у структурі осіб, які їх вчинили [4, с. 34]. Проте, статистична

інформація не завжди об’єктивно відображає кримінальні тенденції у сфері банківської діяльності. На думку 67% опитаних правоохоронців та 58% банківських працівників, рівень участі зацікавлених працівників банку у вчиненні злочинів складає не менше ніж 50%.

Представники банківських установ. До цієї широкої групи ми включили представників державних та недержавних банківських закладів. Усього по вивченим кримінальним справам проходило 79 осіб з числа персоналу банків, що складає 43,8 % від загальної кількості притягнутих до відповідальності за вироком суду. Структура даної групи правопорушників включає у себе: 1) керівники банківських установ чи філій та їх заступники; 2) керівники структурних відділів банківської установи (кредитних та кредитно-фінансових відділів, валютних операцій, інноваційного розвитку тощо) та головні бухгалтери банків; 3) інші працівники банку: кредитні інспектори, економісти, операціоністи, касири, фахівці з інформаційно-програмного забезпечення тощо. Серед представників цієї сфери порівняно високий рівень освіченості: у 87% осіб є вища освіта, з них 53 % - економічна, 28 % - технічна та 19 % юридична.

У структурі названої категорії суб’єктів злочинів 9,7 % осіб складають представники першої підгрупи. Дані про посадовий та соціальний статус винних свідчать про те, що більшість з них займали високе службове становище і мали великі доходи. Вони, як правило, є організаторами (ініціаторами) у вигадуванні схем злочинного збагачення. Як відомо, керівники фінустанов нерідко в імперативному порядку самостійно вирішують питання розподілу банківських ресурсів, мають широкі ділові та особисті стосунки. В силу посадового становища та наявних можливостей, їм доволі часто вдається заплутати сліди своїх злочинних дій та уникнути відповідальності. Підтвердженням тому є опитування представників правоохоронної сфери, де 98,5 % опитаних нами слідчих ОВС України та прокуратури вказали на те, що досить важко довести причетність керівників банків, як організаторів злочинної групи,

до вчинення протиправних дій та приховані слідів від такої діяльності. Такі особи – сильні, добре організовані, розумні, багаті на кошти, кмітливі шахраї, що в змозі коригувати діяльність фінансових установ на свою користь [4, с.35].

Серед чоловіків злочинців-банкірів більше (57 %), ніж жінок. Розподіл за віком відбувся такий: а) 18-24 рр. – 1,7 %, б) 25-29 рр. – 7,4 %, в) 30-45 рр. – 60,7 %, г) від 46 р. і старше – 30,2 %. У цьому списку переважає третя вікова група, як економічно активна, досвідчена і працездатна частина населення. Досвід роботи у банківській сфері серед них, у середньому, складав 7-10 років. Як правило, кожен характеризувався як працелюбний і дуже досвідчений професіонал своєї справи, раніше не був притягнений до кримінальної відповідальності.

Особливу увагу заслуговують представники вікових груп від 18 до 29 років. У їх діях спостерігається висока корисна мотивація до легкої злочинної «наживи» при наявному невеликому досвіді роботи у банках (до 5 років) та відсутності достатніх професійних якостей. Поясненням тому є психологічні особливості віку молодих фахівців, коли є прагнення за короткий термін якомога більше заробити грошей. Тому вони активно включаються до злочинних намірів керівництва, виступаючи співучасниками або посібниками різного роду зловживань на всіх стадіях злочинної діяльності. Такого ж висновку дійшли й соціологи, опитавши у 2009 році в українських компаніях близько 1000 молодих осіб [4, с. 35].

Окремої уваги заслуговують так звані кіберзлочинці. Повна автоматизація та комп’ютеризація банківських операцій, можливості дистанційного доступу до рахунків створюють дуже сприятливі умови для вчинення злочинів у банківській сфері. Особливим «попитом» у даному випадку користуються фахівці у сфері використання комп’ютерних мереж та програмного устаткування. Вітчизняні та зарубіжні дослідження дають змогу намалювати портрет типового «комп’ютерного» злочинця: йому в середньому 30 років, за освітою – інженер у галузі електроніки і

математики, або програміст. Але існують випадки, коли злочинці взагалі не мають ніякої технічної освіти. Крім цього, вказана категорія осіб, як правило, не має кримінального минулого і не знаходиться на обліках в ОВС.

За даними окремих досліджень, суб'єктами злочинів, що вчинюються за допомогою високих технологій, у 5 разів частіше є чоловіки. Більшість злочинців мають вищу технічну освіту (53,7%). В основному це особи вікових груп: від 30 до 45 років (46,5%), а також від 16 до 30 років (37,8%) [**Ошибка! Источник ссылки не найден.**, с. 91]. Вони можуть бути як співробітниками банків, так і працювати в інших господарських структурах (або ж офіційного не працевлаштованими). Кіберзлочинці часто озброєні спеціальними знаннями й найновішими технологіями, мають доступ до банківських комп'ютерних мереж. Частіше за все зазначені особи не тільки володіють спеціальними навичками в сфері користування ЕОМ, їх пристроями, але і можуть користуватися паролями і ключами банківських програм, застосовувати свої спеціальні знання для фальсифікації програмного забезпечення шляхом зміни правильних вихідних даних.

Дослідження показують, що безпосередній несанкціонований доступ до ЕОМ, систем та комп'ютерних мереж вчиняється саме працівниками банків (або колишніми працівниками): програмістами, інженерами, операторами, які є користувачами або обслуговуючим персоналом ЕОМ (41,9%). Майже в два рази менше такий доступ виконують інші працівники банку (20,2%), а в 8,6 % випадків злочин було вчинено співробітниками, що були звільнені, 25,5 % - несанкціонований доступ вчинений сторонньою особою. Найчастіше такі злочинні дії вчиняються у змові.

Так, громадянин П., будучи начальником операційного відділу Полтавської філії АКБ «Укрсиббанк» за попередньою змовою з Х. – директором ДП «Сателіт», зловживаючи службовим становищем вчинили розкрадання грошових коштів клієнтів вказаного банку на загальну суму

195 тис. грн. П., маючи доступ до комп'ютерної інформації вчинив несанкціонований переказ грошей з рахунків фірм-клієнтів банку на рахунки фіктивних фірм, де вони в подальшому були зняті готівкою. Для прикриття злочинної діяльності гр. П., вступивши у змову з Х. та непрацюючим Ф. викрав зразки підписів та печаток фірм-клієнтів, підробив низку платіжних документів. Дії зазначених осіб отримали кваліфікацію у суді за ст.ст. ч. 2 ст. 191, ч.5 ст. 200, ч.2 ст. 366, ч.2 ст.15, ч.2 ст. 362, 358, та 209 КК України [5, с.17].

Особливу небезпеку представляють випадки входження у змову з керівниками підрозділів і служб самої комерційної структури або пов'язаних з нею систем, а також з організованими злочинними групами, оскільки заподіювана матеріальна шкода від вчинених злочинів значно збільшується. Близько 90% зловживань у банківській сфері, пов'язаних з порушеннями в області інформаційної безпеки, відбувається за прямої або непрямої участі діючих або колишніх працівників банків. При цьому на злочинний шлях часто стають найбільш кваліфіковані з них, саме ті, які володіють значущою інформацією про програмні системи банку – системні адміністратори й інші співробітники служб автоматизації банків.

З урахуванням вищенаведеного можна стверджувати, що представники банківської сфери вчиняють злочини групою осіб, і дуже рідко – одноособово: 92,1 % проти 7,9 % відповідно. Взаємодіючи один з одним вони утворюють різні форми співпраці у процесі підготовки, вчинення злочину, приховані слідів чи забезпеченні «прикриття» злочинної діяльності. У ланцюгу злочинних дій, об'єднаних спільною метою, суб'єкти злочинів, в залежності від статусу та розподілу ролей, вчиняють основні чи допоміжні злочини, виступають ініціаторами, організаторами, учасниками, співучасниками чи посібниками у вчиненні злочинних дій.

Вивчаючи організовану злочинну діяльність у банківській сфері, треба визначити, що злочинні групи розрізнюються по кількісному складу,

ступеню організованості, рівню підготовки та досвіду. У цьому зв'язку їх можна розподілити на дві класифікаційні групи:

1) ситуативні або не стійкі злочинні об'єднання (групи);

2) стійкі організовані злочинні групи (злочинної організації).

Перша група включає у себе, як правило, невеликий склад учасників (до 4-5 чоловік). Для цієї групи не є характерним високий ступень організованості її учасників. Об'єднанні спільною метою, злочинці не ставлять за мету вигадування складних схем злочинного збагачення та отримання систематичного кримінального доходу. Як показує слідчо-судова практика такі групи найчастіше зустрічаються у технології злочинного збагачення шляхом незаконного отримання та розкрадання кредитних ресурсів банку (40,5% випадків), та у технології розкрадання безготівкових грошових коштів клієнтів банку з використанням фіктивних розрахункових документів та електронно-обчислювальної техніки (27,5% випадків).

Така злочинна група може утворитися: суто з банківських працівників, може бути змішаною (об'єднання банкірів з посадовими особами інших суб'єктів господарювання), а також виключно з представників небанківського сектору (приватних підприємців, фізичних осіб тощо).

Діяльність другої групи уявляє собою стійке злочинне об'єднання, яке спрямоване на вигадування складних схем та технологій злочинного збагачення з метою системного отримання кримінального прибутку. До складу цієї групи входить широкий спектр представників сфери господарювання та органів влади, яких привертає увагу, перш за все, перспектива систематичного безкарного одержання злочинним шляхом величезних коштів через використання корупційних зв'язків. У такій організованій злочинній групі характерним є старанна підготовка до скоєння злочинів та приховані слідів. Вона включає у себе розроблення плану, розподілення функцій між окремими членами групи, коли кожний з

них виконує тільки свою частку злочинної «роботи». Для цієї групи також характерні: професіоналізм та обізнаність учасників; змобілізованість їхніх дій; психологічна та субкультурна сумісність членів групи, їх спеціалізація; конспіративність функціонування; регенерація кримінальних ланок; чіткий розподіл злочинних прибутків, проникнення у широкий спектр сфер легальної та тіньової економічної діяльності; потужні кримінальні зв'язки з представниками органів влади та управління тощо. Діяльність цієї групи може носити транснаціональний характер.

Матеріали слідчо-судової практики вказують, що діяльність членів другої класифікаційної групи в основному зосередження в складних технологіях злочинного збагачення. Елементами останньої, як правило виступають наявність мережі фіктивних фірм та банків, що діють у складі КЦ. Легалізація доходів, отриманих злочинним шляхом являється обов'язковим етапом у ланцюгу кримінального циклу задля продовження існування та розвитку діяльності організованої злочинної групи.

3. Організація розслідування фактів злочинного збагачення шляхом несанкціонованого доступу до систем дистанційного обслуговування клієнтів банку

Досудове слідство по злочинам даної категорії починається за умов отримання законних приводів і підстав, що вказують на наявність у діях осіб ознак того чи іншого злочину. Як правило, факти несанкціонованого доступу до рахунків клієнтів банку та подальшого розкрадання коштів виявляються:

1) оперативними підрозділами (податковою міліцією, підрозділами ДСБЕЗ, УБОЗ, СБУ) у ході проведення оперативно-розшукової діяльності;

2) слідчими в ході кримінального провадження про інший злочин.

Також про зазначені злочини може стати відомо із заяв представників фінансової установи (банку), повідомлень ЗМІ, заяв громадян і повідомлень службових осіб контролюючих органів.

Вже на стадії відкриття кримінального провадження ознаки повинні бути зіставлені з елементами складу злочину, передбаченого кримінально-правовою нормою. При отриманні даних про злочинні дії важливе місце займає аналіз перевірки первинних матеріалів, а саме:

Матеріали оперативно-розшукових підрозділів у яких повинні бути узагальнюючі дані про проведену оперативно-розшукову роботу з виявлення і документування фактів несанкціонованого втручання у ЕОМ та незаконного переказу грошових коштів клієнтів банку.

Заява та письмове пояснення від потерпілої сторони (як правило, це особа від керівництва банківської установи) про факт протиправної діяльності та заподіяної шкоди. Зазвичай у заяві потерпілі також обмежуються лаконічним викладенням суті вчинених протиправних дій, оскільки більш докладна інформація міститься в їх поясненнях.

Письмові пояснення очевидців протиправних дій. Це можуть бути пояснення як представників банківської установи (головний бухгалтер банку, керівництво та працівники кредитного, валютного, розрахункового відділів, відділу інформаційно-програмного забезпечення тощо), так і представників підприємницьких структур чи фізичних осіб з приводу встановлених порушень або інших обставин злочину. Також долучаються свідчення, що спростовують причетність окремих осіб до події злочину.

Документи (копії) від банківських установ, які є підтвердженням злочинних дій*:*

- що були використанні як засіб вчинення злочину;
- що послугували засобом приховання злочину;
- що є предметом злочину.

Це можуть бути дійсні або підроблені бухгалтерські, розрахунково-банківські й інші документи, що відображають окремі бухгалтерські

операції, рух грошей, матеріальних цінностей (банківські баланси дня, форми фінансової звітності, меморіальні ордери банківського обліку, документи з кредитної справи, договори на відкриття поточного або депозитного рахунків, угоди на розрахунково-касове обслуговування, акредитиви, платіжні доручення /вимоги/, виписки за поточними рахунками, аналіз руху грошей, платіжні доручення тощо).

Тимчасово вилучена техніка (носії інформації – вінчестери, диски, флеш-накопичувачі, тощо), яка слугувала знаряддям вчинення чи приховання злочину, або зберегла на собі сліди злочинних акцій.

Матеріали спеціальних перевірок. До вказаних матеріалів входять: акти документальних ревізій підрозділів фінансової інспекції України, інспекційні перевірки НБУ щодо дотримання порядку здійснення операцій з іноземною валютою, матеріали ревізійних комісій комерційних банків, висновки незалежних аудиторів, довідки про проведені дослідження фахівцями в галузі бухгалтерського обліку, аудиту, фінансів та комп'ютерної техніки тощо.

Письмове пояснення особи (осіб), що підозрюються у вчиненні злочину про факти вчинення протиправних дій. Наявність пояснень забезпечує об'єктивність та неупередженість оцінки первинного матеріалу щодо наявності ознак злочину (або інших правопорушень). Крім того, вони мають важливе тактичне значення, оскільки певною мірою дозволяють спрогнозувати можливу поведінку підозрюваного під час слідства, визначити його лінію захисту та позицію (активне протистояння або часткова співпраця). Більше того, пояснення може містити дані про інших співучасників, їх роль у протиправній діяльності. Зрозуміло, що порушнику невигідно давати пояснення щодо інших епізодів своєї злочинної діяльності або участі інших осіб, оскільки це веде до обтяження кримінальної відповідальності. Тому висновки про можливий зв'язок злочину з іншими злочинами слідчому доведеться робити, виходячи з

механізму злочину (технології злочинної діяльності) та представлених даних.

Інші документи – це можуть бути запити до відповідних наглядових установ, звернення, листи, чорнові записи, рапорти про проведення оперативних та розшукових заходів, рішення судів у рамках цивільного або господарського провадження тощо.

Зазначений перелік документів не є вичерпним, але в ньому відображається типова структура первинних матеріалів перевірки інформації про злочини у сфері, що розглядається. Винесенню процесуального рішення за матеріалами дослідчої перевірки передує оцінка отриманих даних. У кожному конкретному випадку слідчий може судити про наявність або відсутність підстави для ухвалення процесуального рішення лише після оцінки отриманої в ході дослідчої перевірки криміналистично значимої інформації. До такої інформації відноситься інформація про криміналістичні ознаки злочину: типові сліди, особистість злочинця, обставини здійснення злочину й інші фактичні дані, які мають значення для початку кримінального провадження та дозволяють висувати визначені версії.

До *обставин*, що підлягають оцінці на стадії початку досудового слідства, варто відносити: кримінально-правові ознаки кваліфікованого складу економічного злочину; криміналістичні ознаки діяльності організованої злочинної групи; достатність даних, що вказують на ознаки злочинних технологій, час, місце, здійснення і матеріальні наслідки.

Якщо слідчому або оперативному працівнику стало відомо про кілька фактів вчинення злочинів певною особою, необхідно встановити зв’язок між цими фактами, вирішити питання про заведення кримінальних справ щодо інших осіб.

При розслідуванні злочинів в даній сфері можливо виділити три типові слідчі ситуації:

1. Злочин, пов’язаний з рухом комп’ютерної інформації, вчинений в умовах очевидності – характер і його обставини відомі (наприклад, яким способом введено в комп’ютерну мережу) і виявлені потерпілим власними силами, злочинець відомий і затриманий;

2. Коли відомий спосіб вчинення, але механізм злочину у повному обсягу не зрозумілий. Наприклад, стався несанкціонований доступ системи ДБО через слабкі місця в захисті комп’ютерної мережі. Злочинець відомий, але переховується;

3. Коли в наявності злочинний результат, наприклад дезорганізація комп’ютерної мережі банку. Механізм же злочину і злочинець невідомі.

У першому випадку необхідно встановити, чи був причинно-слідчий зв’язок між несанкціонованим проникненням в комп’ютерну мережу та наслідками (збоями в роботі, занесенням комп’ютерного вірусу та інше), встановити розміри збитків. В другому випадку – першочерговим завданням, поряд з наведеними вище, є розшук та затримання злочинця. І нарешті, в найменш сприятливому (третьому) випадку необхідно встановити механізм злочину.

3.1. Особливості дій слідчо-оперативної групи у приміщенні комерційного банку

Керівник слідчо-оперативної групи має заздалегідь підготуватися до проведення слідчих дій у приміщенні комерційного банку. Необхідно ретельно вивчити територіальне розташування банку, визначити в якому приміщенні банк знаходиться: у вбудованому, прибудованому, окремо розташованій будівлі, вивчити входи-виходи (основні й запасні), кількість місцезнаходження пунктів обміну валют.

Необхідно чітко визначити розташування внутрішніх приміщень банку: сховища; спеціальної каси; каси перерахунку; вечірньої каси; операційного залу; центру автоматизованої обробки інформації

(комп'ютерного центру-серверу, архівування, модему «Банк – клієнт»); приміщень, де знаходяться індивідуальні сейфи для зберігання цінностей; кабінетів керівництва банку, головного бухгалтера (знати в яких кабінетах працюють комп'ютери, які включено в мережу); підсобних приміщень, особливо приміщень перед сховищами (їх треба оглядати ретельно); складських приміщень.

Приступивши до виконання слідчих дій у банку необхідно:

1) ретельно вивчити план приміщення банку з розташуванням всіх внутрішніх кабінетів (безпосередньо на місці);

2) за необхідності забезпечити охорону основних і запасних входів та виходів;

3) ознайомитися з документами, що визначають організаційну структуру банку, положенням про управління (відділи), наказом про розподіл обов'язків між керівництвом, ліцензією на здійснення операцій видану НБУ;

4) забезпечити присутність посадових осіб банку, а в окремих випадках – присутність представників НБУ.

Огляд управління (відділу) автоматизації. Зазначений відділ є особливим підрозділом, який працює на зв'язку з розрахунковою палатою НБУ і в якому обліковуються всі витратні операції банку. Керівнику слідчо-оперативної групи бажано досконало знати комп'ютерну програму, яку використовує банк у своїй роботі.

Також треба звернути увагу на роботу головного комп'ютера, який контролює усі фінансові операції банку. Витратні операції клієнтів, як правило, здійснюються після обіду, а вдень активно працюють грошові ресурси фіктивних фірм. У банку також може знаходитися комп'ютер «фіктивної» фірми, коли ця фірма обслуговується за договором по системі «клієнт-банк» (на це треба звернути особливу увагу).

Під час проведення слідчих дій необхідно:

1) забезпечити присутність працівників на своїх робочих місцях (не допускати відходу з робочого місця жодного з працівників);

2) здійснювати ретельний контроль за касирами (буквально, за рухами рук, місцем знаходження їх особистих речей (сумок));

3) контролювати дії працівників центру автоматизованої обробки інформації, не допускаючи здійснення операцій в момент проведення слідчих дій, а також усіх працівників, які працюють за комп'ютерами, що включені в мережу;

4) оглянути приміщення банку на предмет виявлення комп'ютерної техніки, яка може «нелегально» працювати від імені фіктивної фірми;

5) спостерігати за телефонним зв'язком, бо працівник банку може дати команду про списання коштів з будь-якого рахунку банківської установи чи підприємства;

6) забезпечити зовнішнє спостереження за банком (вікнами) і внутрішню охорону входу-виходу основного й запасного, забезпечуючи тільки вхід бажаючих до банку;

7) у ході огляду в приміщені операційного залу швидко виявити за роздруківкою фіктивні фірми за такими ознаками: фірми з великими оборотами, що почали працювати протягом останнього часу (від 1-3 днів до 2-3 місяців). Після встановлення осіб директора та головного бухгалтера цих фірм визначити відповідність даних, що знаходяться в банку за даними адресного бюро (чи не були раніше загублені чи викрадені документи, що пред'явлені при відкритті рахунку). Перевірити, чи знаходиться фірма за юридичною адресою відповідно до банківських документів.

8) у разі виникнення підозри необхідно відразу припинити рух безготівкових коштів в частині проведення витратних операцій на рахунках банку (поточних, розрахункових, депозитних; у національній валюті, іноземній валюті) одночасно по всім підрозділам.

Припинення руху безготівкових грошових коштів у частині витратних операцій дасть можливість проведення перевірки та виявлення наявності всіх грошових коштів банку і підприємств, які обслуговуються в цьому банку, – дійсних та фіктивних. У такому випадку у керівництва банку не буде можливості у присутності перевіряючих провести операції, підганяючи таким чином, під облік наявність ресурсів банку та вивести кошти фіктивних фірм з банку.

Таким чином, алгоритм дій співробітників оперативно-слідчої групи дозволяє чітко визначити мету перевірки комерційного банку, що, у свою чергу, дозволить визначити певні напрями збору оперативної інформації. Тобто оперативні працівники чітко усвідомлять, яку інформацію та документи необхідно шукати з метою їх підтвердження при безпосередній перевірці кредитно-банківської установи.

Необхідно знати **особливості тактики окремих слідчих дій**, в ході яких здійснюється виявлення, фіксація, вилучення комп'ютерної інформації, а саме: огляду місця події (місцевості, приміщень, предметів, документів), обшуку (в тому числі особистого, на місцевості та в приміщенні), виїмки (предметів, документів, поштово телеграфної кореспонденції, документів, що містять державну таємницю), прослуховування телефонних і інших переговорів. При виконанні цих слідчих (гласних та негласних) дій необхідно тактично правильно проводити пошук комп'ютерної інформації, що дозволяє уникнути її знищення чи пошкодження; знайти необхідне; зафіксувати і вилучити його у відповідності з процесуальними нормами. Сучасний розвиток електроніки дозволяє зберігати велику кількість інформації в незначних за обсягом приладах. При підготовці до огляду, обшуку чи виїмки слідчий вирішує питання про необхідність вилучення комп'ютерної інформації. На цю необхідність, крім ознак складу злочину в сфері руху комп'ютерної інформації, можуть вказувати:

- наявність у підозрюваного (обвинуваченого) чи потерпілого (у деяких випадках свідка) спеціальної освіти в області обчислювальної техніки, а також комп'ютерної техніки в особистому користуванні;

- присутність в матеріалах справи документів, виготовлених машинним способом (відповіді на запити, довідки, отримані від обвинуваченого чи потерпілого);

- викрадення носіїв комп'ютерної інформації;

- свідчення про захоплення вищевказаних осіб комп'ютерною технікою, програмуванням або про їх часті контакти з особами, що мають такі захоплення.

На підготовчому етапі огляду чи обшуку необхідно отримати достовірні данні про вид та конфігурацію ЕОМ, що використовується; про те, чи підключена вона до локальної чи глобальної мережі (Інтернет); наявності служби інформаційної безпеки і захисту від несанкціонованого доступу; системи електроживлення приміщень, де встановлена комп'ютерна обчислювальна техніка; кваліфікацію користувачів; зібрати відомості про співробітників, що обслуговують комп'ютерну техніку (взаємовідносини в колективі, його можливої криміналізації та інше). Володіння такою інформацією забезпечить слідчому доступ до інформації, що зберігається в комп'ютері та максимально підвищить її доказову силу.

В багатьох випадках вирішальне значення має раптовість обшуку (невідкладність огляду), оскільки комп'ютерну інформацію можливо швидко знищити. Якщо отримані свідчення про те, що комп'ютери організовані в локальну мережу, слід завчасно встановити місце знаходження всіх засобів комп'ютерної техніки, що підключені до даної мережі та організувати груповий обшук одночасно у всіх приміщеннях де встановлено ЕОМ. Перед початком обшуку (огляду) вживають заходи, які попередять можливість пошкодження чи знищення інформації. Для цього слід забезпечити контроль за безперебійним електроживленням ЕОМ в момент огляду, вивести всіх сторонніх осіб з території, на якій

проводиться огляд чи обшук, перекрити подальший доступ людей; вжити заходів для того, щоб особи, що залишилися не мали можливості торкатися до засобів комп'ютерної техніки і джерел електроживлення. Огляд чи обшук доцільно проводити з участю спеціаліста в області інформатики і обчислювальної техніки. Бажано в якості понятих запрошувати осіб, що знайомі з роботою ЕОМ.

Не слід обмежуватися пошуком інформації тільки в комп'ютері. Необхідно уважно оглянути документацію, що мається (навіть у записах на обривках паперу, оскільки програмісти часто, не сподіваючись на свою пам'ять залишають записи про паролі, зміну конфігурації системи, особливості будування інформаційної бази комп'ютера). Велика кількість користувачів зберігають копії своїх файлів на дискетах для уникнення їх втрати при виході комп'ютеру із ладу. Тому будь-які виявлені носії інформації повинні бути вилучені і вивчені.

Тактика пошуку комп'ютерної інформації повинна обиратися виходячи з ступеню захисту даних та функціонального стану комп'ютера і периферійних приладів на момент проведення слідчої дії.

Про високий ступень захисту комп'ютера може свідчити наявність спеціальних систем захисту інформації від несанкціонованого доступу і (або) сертифікованих засобів захисту; постійна охорона території і будівлі, де розміщена комп'ютерна система, за допомогою технічних засобів і спеціального персоналу, використання суворого пропускного режиму, спеціального обладнання приміщень; наявність адміністратора (служби) захисту інформації, нормальне функціонування і контроль роботи.

Низький ступень захищеності визначається наявністю простого алгоритму обмеження доступу (наприклад, дані захищені тільки паролем), отриманням достовірних даних про його подолання, при цьому немає необхідності застосовувати спеціальні засоби доступу до інформації.

Діяльність слідчого при подоланні захисту комп'ютера від несанкціонованого доступу - одна з самих відповідальних. Саме при

некоректному поводженні захищені дані можуть бути самознищені, перекручені, сховані і за допомогою спеціальних програм. Для того щоб цього не відбулося при підготовці до проведення слідчої дії необхідно якомога точно і повно визначити ступінь захищеності комп'ютера, засоби захисту, паролі, ключові слова і т.д.

З одного боку, більшість спеціалістів вважають, що в сфері обчислювальної техніки та програмування на сьогоднішній день немає програмно-технічних засобів, які здатні на сто відсотків гарантувати захист. Звідси виходить, що в принципі, можливо подолати будь-яку перешкоду при пошуку інформації. З іншого боку, існують засоби захисту, в яких використовують різноманітні алгоритми і принципи будови захисту, такі що для їх подолання може знадобитися чимало часу. Серед хакерів саме подолання захисту від несанкціонованого доступу являється одним з найвищих підтверджень майстерності.

Захист комп'ютерної інформації здійснюється шляхом ідентифікації (користувач повідомляє своє ім'я) і автентифікації (перевірки справжності) – інша сторона впевнюється, що суб'єкт дійсно той, за кого себе видає. Справжність підтверджується знанням пароля, особистого ідентифікаційного номеру, криптографічного ключа та інше; особистою карткою або іншим приладом аналогічного призначення; голосом, відбитками пальців і іншими біометричними характеристиками і т.д.

Паролі, які давно вбудовані в операційні системи і інші сервісні програми при правильному використанні можуть забезпечити рівень безпеки, що підходить для багатьох організацій. Але, за сукупністю характеристик їх слід визнати найбільш слабким засобом перевірки справжності. Надійність паролів полягає в здатності запам'ятати їх та зберігати в таємниці.

Аналіз парольного захисту при огляді або обшуку комп'ютерної техніки дозволяє слідчому з великою вірогідністю визначити істинного власника криміналістично-значимої інформації, яка знайдена в комп'ютері.

Іншими словами, чим вище надійність парольної системи, тим з більшою імовірністю можливо визначити її істинного власника і тим вища доказова сила виявленої інформації.

Іншим засобом автентифікації служать **токени** – предмети або прилади, володіння якими підтверджує справжність користувача. Найпоширенішими з них являються картки з магнітною смугою. Зазвичай користувач набирає на клавіатурі свій ідентифікаційний номер, після чого процесор перевіряє його співпадання з тим, що записано на карточці, а також справжність самої картки.

До перерахованих засобів також потрібно віднести і електронні ключі. Електронний ключ – прилад з пам'яттю, виконаний на спеціалізованій мікросхемі, розміром не більше коробки сірників. Якщо при огляді комп'ютера запустити захищену програму, то вона перевіряє наявність свого ключа. Коли такий ключ знайдено, програма виконується. В іншому випадку видається інформація про помилку і робота припиняється. Сам ключ вводиться в порт комп'ютера, що призначений для підключення принтера і легко виводиться.

Однак успішне подолання захисту ще не вирішує всі проблеми збору доказів в комп'ютері. Тактичні особливості пошуку комп'ютерної інформації залежать також від функціонального стану ЕОМ і периферійних приладів на момент огляду чи обшуку. Інформація може бути або зафіксована на постійному носію, або зберігатися в ЕОМ тільки в період її роботи, тому слідчому необхідно обирати різні тактичні прийоми пошуку у залежності від того працює комп'ютер на момент слідчої дії чи відключений.

При вмиканні комп'ютера в роботу електронні прилади утворюють в ньому певний обсяг так званої оперативної пам'яті (ОЗУ), яка призначена для операційних дій над інформацією і програмами та зберігає їх в процесі роботи. При вимиканні комп'ютера або закінченні роботи з конкретною програмою чи даними ОЗУ очищується і готове для вводу нових. В процесі

роботи комп’ютера ОЗУ спеціальними програмними засобами розмежовується на спеціальні області, призначені для окремого зберігання програм і даних. Серед таких областей, по бажанню користувача, може бути виділена спеціальна, яка імітує зовнішній прилад – накопичувач інформації. Цей накопичувач (так званий “віртуальний диск” чи “псевдодиск”) відрізняється високою швидкістю доступу і дозволяє виконувати специфічні операції по обміну програмами (даними) з приладами ЕОМ. Про робочий стан комп’ютера свідчить положення тумблерів, мерехтіння чи горіння індикатерів на передній панелі системного блоку, зображення на моніторі, невелика вібрація і ледь чутний шум працюючих в середині вентиляторів.

У випадку, коли комп’ютер на момент початку огляду виявився ввімкненим, необхідно оцінити інформацію, що зображена на моніторі. По-перше, встановити яка програма виконується на даний момент. У випадку роботи стандартного програмного продукту (наприклад, на екрані зображені вікна операційних оболонок Norton Commander чи Windows) – не виконувати будь-які маніпуляції на вході без попереднього візуального огляду технічних засобів. Екран монітора необхідно сфотографувати. Відключити всі телефонні лінії, що з’єднані з комп’ютером. Описати всі з’єднання на задній стінці системного блоку. Якщо необхідно, відкрити кожух системного блоку та візуально визначити конфігурацію ЕОМ, описати місцезнаходження електронних плат. Дотримання даних правил дозволить зробити безпечним пошук інформації від різноманітних приладів пошкодження та знищення як апаратних засобів, так і інформаційної бази. Цими засобами можуть бути електронні ключі, радіозакладки і т.д. У випадку, якщо при огляді апаратних засобів виявлені невідомі учасникам огляду (обшуку) прилади (плати розширення, нетипові з’єднання і т.д.), комп’ютер необхідно одразу виключити. При цьому слід не відключати тумблер блоку живлення, а витягнути вилку з розетки. Потім (до відключення проводів) необхідно промаркувати всю систему

підключення, всі порти і роз’єми, щоб потім було можливо здійснити точну реконструкцію розміщення кабелю, плат розширення та інших приладів.

Якщо конфігурація процесору стандартна, потрібно коректно завершити роботу виконаної програми. Або дочекатися завершення її роботи до видачі додаткових, можливо пошукових даних. Особам, які присутні при огляді (обшуку) необхідно роз’яснити всі дії слідчого і спеціаліста у ході маніпуляції з ЕОМ. Неприпустимо втручання в інформаційну базу без наглядного і доступного коментарю своїх дій. Повинен бути пояснений будь-який натиск на клавіатуру, пересування миші і т.п.

Якщо при пошуку інформації задіються програмні продукти, які не знаходяться в комп’ютері, але використовуються слідчим, це необхідно відмітити у протоколі огляду або обшуку. Максимально активна участь понятих при пошуку інформації важлива тому, що результатом виконання пошуку може з’явитися не текстовий або графічний документ, а аудіо-, відеоролик (вербальна або візуальна інформація). Такий підсумок роботи програми, будучи унікальним (неповторним), фіксується за допомогою протоколу (не враховуючи фото- і відеозапис).

У разі коли інформація буде знайдена, поточне зображення екрану дисплея необхідно сфотографувати, після чого стандартними засобами переписати інформацію на постійний носій (зазвичай – магнітний диск) або роздрукувати.

Вмикати і вимикати комп’ютери, виконувати з ними будь-які операції може спеціаліст в галузі обчислювальної техніки. Якщо на об’єкті було відключене електропостачання, наприклад, в зв’язку з пожежею або вибухом, до його вимикання слід перевірити чи знаходяться всі комп’ютери і периферійні прилади у вимкненому стані. Вилучати необхідно відразу всі, комп’ютери (або хоча б блоки пам’яті) і магнітні носії, що маються на об'єкті. Не допускається залишати їх для зберігання

на самому об'єкті чи в іншому місці, де до них можуть мати доступ сторонні особи. Інформація, що міститься на магнітних носіях, може бути легко знищена злочинцем, наприклад, за допомогою джерела електромагнітного випромінювання. При цьому візуально виявити це не можливо.

Комп'ютери і їх комплектуючі опечатуються: на роз'єми накладають лист паперу, закріплюючи його краї на бокових стінках комп'ютера густим клеєм або клейкою плівкою, для того щоб виключити можливість роботи з ним у відсутність власника чи експерта.

Магнітні носії поміщаються, зберігаються і транспортуються в спеціальних екранованих контейнерах чи в стандартних футлярах заводського виготовлення, для того щоб виключити руйнівну дію різних електромагнітних і магнітних полів і направлених опромінювань. Опечатуються тільки контейнери чи футляри. Пояснювальні надписи наносяться на спеціальні етикетки для дискет.

В протоколі слідчої дії описуються основні фізичні характеристики приладів, магнітних і інших постійних носіїв інформації, що вилучаються, серійні номери апаратури, їх видимі індивідуальні ознаки, машинні роздруківки оформлюються як додаток до протоколу.

При здійсненні **допитів** підозрюваних і обвинувачених необхідно враховувати дані криміналістичної характеристики про особу злочинця. Важливою є підготовка до допиту, в процесі якої необхідно намагатися хоча б умовно обрати до якої групи відноситься підозрюваний чи обвинувачений, і на цьому засновувати тактику допиту. При початковому допиті необхідно, спонукаючи особу до дійового каяття, з'ясувати:

- які зміни в роботу комп'ютерних систем були внесені;
- які віруси використовувалися;
- чи є з точки зору підозрюваного (обвинуваченого) можливість швидко усунути чи зменшити шкоду, що спричинена внаслідок несанкціонованого проникнення в систему;

- які відомості і кому передавалися.

При початкових допитах свідків і потерпілих необхідно з'ясовувати:

- призначення і функції комп’ютерної системи;
- хто мав доступ до неї і в приміщення, де знаходилась комп’ютерна техніка;
- чи не з'являлися там сторонні особи;
- які засоби захисту використовувалися;
- якщо частина інформації була закритою, то хто санкціонував доступ до неї і хто реально був допущений;
- яка шкода (майнова та немайнова) завдана злочином і чи є способи її зменшити.

3.2. Призначення судових експертиз

Як вже зазначалося, велике значення має у справах даної категорії участь спеціаліста в збиранні доказової інформації. Але найбільш значимий її подальший аналіз, досліджування доказів в ході проведення експертиз.

Основний напрям проведення експертиз це – комп’ютерно-технічний. У відповідності з завданнями і специфікою об’єктів дослідження на теперішній час в рамках цього роду експертиз можливо виділити такі види:

- **технічні експертизи комп’ютерів і їх комплектуючих** (судова комп'ютерно-технічна експертиза: апаратно-комп’ютерна та комп`ютерно-мережева), які проводяться з метою вивчення конструктивних особливостей і стану комп’ютера, його периферійних приладів, магнітних носіїв, комп’ютерних мереж, а також причин виникнення порушень в роботі;

- **експертизи даних і програмного забезпечення** (програмно-комп'ютерна, інформаційно-комп'ютерна судові експертизи), які

здійснюються з метою вивчення інформації, що зберігається в комп'ютері і на магнітних носіях.

Питання, які виносяться на вирішення комп'ютерно-технічної експертизи, по її виду можливо розділити також на дві групи. Питання, які вирішуються технічною експертизою комп'ютерів і їх комплектуючих (діагностичні):

1) комп'ютер якої моделі наданий на дослідження; які технічні характеристики його системного блоку і периферійних приладів; які технічні характеристики даної обчислювальної мережі;

2) де і коли виготовлений і зібраний даний комп'ютер і його комплектуючі; складання комп'ютера здійснювалось в заводських або кустарних умовах;

3) чи співпадає внутрішня будова комп'ютера і периферія запропонованій технічній документації; чи не внесені в конструкцію комп'ютера зміни (наприклад, установка додаткових вбудованих приладів: вінчестерів, приладів для розширення оперативної пам'яті, зчитування оптичних дисків, інші зміни конфігурації);

4) чи справний комп'ютер і його комплектуючі; який їх знос; які причини несправності комп'ютера і периферійних приладів; чи містять фізичні дефекти носії інформації;

5) чи проводилась адаптація комп'ютера для роботи з специфічним користувачем (лівша, людина з вадами зору та інші);

6) які технічні характеристики інших електронних засобів прийому, накопичення і видачі інформації (електронна записна книжка, телефонний сервер); чи справні ці засоби; які причини поломки.

Питання, які вирішуються експертизою даних і програмного забезпечення (*діагностичні*):

1) яка операційна система використана в комп'ютері;

2) який зміст інформації, що зберігається на внутрішніх і зовнішніх магнітних носіях, в тому числі, які програмні продукти там

знаходяться; яке призначення програмних продуктів; який алгоритм їх функціонування, способу вводу і виводу інформації; який час проходить з моменту вводу даних до вводу результатів при роботі з даною комп'ютерною програмою, бази даних;

3) чи являються дані програмні продукти ліцензованими (або несанкціонованими) копіями стандартних систем чи оригінальними розробками;

4) чи вносилися в програму даного системного продукту будь-які корективи (які), що змінюють виконання деяких операцій (яких);

5) чи співпадає даний оригінальний комп'ютерний продукт технічному завданню; чи забезпечується при його роботі виконання всіх передбачених функцій;

6) чи використовувалися для обмеження доступу до інформації паролі, приховані файли, програми захисту та інше; який зміст прихованої інформації; чи відбувалися спроби підбору паролю, злому технічних засобів та інші спроби несанкціонованого доступу;

7) чи можливе відновлення стертих файлів, дефектних магнітних носіїв інформації; який зміст відновлених файлів;

8) який механізм втрати інформації із локальних обчислювальних мереж і розподілених баз даних;

9) чи маються збої у функціонуванні комп'ютера, роботі окремих програм; які причини цих збоїв; чи не викликані збої в роботі комп'ютера впливом вірусу (якого); чи поширюється негативний вплив вірусу на більшість програм, чи він діє тільки на визначені програми; чи можливо відновити в повному обсязі функціонування даної програми (текстового файлу), пошкодженої вірусом;

10) який зміст інформації зберігається в електронній записній книжці та інше; чи зберігається в книжці прихована інформація і який її зміст;

11) коли проводилось останнє корегування даного файлу або інсталяція даного програмного продукту;

12) який був рівень професійної підготовки в галузі програмування і роботи з комп'ютерною технікою особи, яка виконувала дані дії.

За допомогою комп'ютерно-технічних експертиз можливе вирішення деяких питань *ідентифікаційного* характеру:

1) чи мають комплектуючі комп'ютера (плати, магнітні носії, дисководи та інше) єдине джерело походження;

2) чи не написана дана комп'ютерна програма певною особою (вирішується комплексно при проведенні комп'ютерно-технічної і авторознавчої експертиз).

Об'єктами комп'ютерно-технічної експертизи виступають:

- зібрані комп'ютери, їх системні блоки;

- периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, та інше), комунікаційні прилади комп'ютерів і обчислювальних мереж;

- магнітні носії інформації (жорсткі диски і зовнішні накопичувачі, оптичні диски);

- роздруківка програмних і текстових файлів;

- словники пошукових ознак систем (тезауруси), класифікатори та інша технічна документація, наприклад технічні завдання і звіти;

- електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них.

3.3. Особливості проведення тактичних операцій

Відповідно до завдань початкового етапу кримінального провадження можна розглянути наступні тактичні операції: «Усунення

протидії» та «Встановлення причетності банківського працівника до вчинення злочину».

Тактична операція *«Усунення протидії досудовому слідству»*. Таку протидію слід сприймати як певною мірою природне явище. Це випливає із самої сутності правоохоронної діяльності, для якої характерно подолання опору з боку осіб, незацікавлених у встановлені істини. Агресивний настрій відносно слідчих чи оперативних працівників не обов'язково вказує на ймовірних злочинців. Причиною подібної поведінки, як правило, є загальні тенденції у суспільстві. Більш того, такі конфліктуючі представники банківської установи можуть володіти цінною доказовою інформацією про подію злочину. Тому слідчий повинен мати певні творчі здібності, щоб подолати конфліктну ситуацію й одержати цікаві відомості законним шляхом.

Форми (види) протидії проведенню досудового слідства розділяються на дві групи: прихована від слідчого та відкрита (явна) протидія. Прихована протидія може здійснюватися шляхом неповідомлення відомостей, наданні неправдивих показань, підкупу свідків, поширення неправдивої інформації, залякування та здійснення іншого впливу на свідків. Завдання слідчого у даному випадку полягає в нейтралізації всіх фактів такої протидії.

Надання неправдивих показань є найбільше часто використовуваною формою протидії. Як правило, працівники банку (особливо представники керівництва), що причетні до вчинення зловживань, при його підготовці передбачають можливість їх допиту, і тому заздалегідь продумують можливі пояснення щодо виявлених порушень. Викрити допитуваного у наданні неправдивих показань можна лише шляхом послідовного пред'явлення зібраних доказів. Доцільно за кожним фактом, що став об'єктом перевірки, представляти допитуваній особі документи, які свідчать про протиріччя в його показаннях. Також дуже важко буває

виявити факт підкупу свідків. Вони теж ретельно продумують показання, які будуть давати слідчому при допиті.

Не секрет, що сучасна банківська система має потужні корумповані зв'язки з представниками влади. Власники багатьох вітчизняних банків володіють можливостями перешкоджання об'єктивному та повному проведенню кримінального розслідування. Уникнути подібної протидії можна шляхом проведення досудового слідства в особливому режимі, що унеможливлює виток інформації та будь-якого виду впливу на слідчого й інших учасників процесу. Враховуючи вищесказане, необхідно використовувати в процесі досудового слідства єдиний комплекс заходів, умовно називаний «роботою в умовах ізоляції».

Ізоляція працівників слідчо-оперативної групи на час кримінального провадження дозволяє забезпечити їх безпеку, а також збереження отриманої інформації. Ефективна ізоляція може бути досягнута шляхом проведення таких заходів:

1) скорочення до мінімуму контактів співробітників слідчої оперативної групи з особами, що не мають відношення до справи;

2) проведення більшої частини допитів і очних ставок на території органа внутрішніх справ чи прокуратури;

3) одночасна присутність декількох представників слідчої оперативної групи при проведенні слідчих дій за участю представників банку чи іншої установи, де проводяться слідчі дії;

4) у виключних випадках, при проведенні відповідальних слідчих дій, створення «груп забезпечення» із числа співробітників спецпідрозділів міліції з метою забезпечення безпеки співробітників слідчої оперативної групи.

Тактична операція *«Встановлення причетності банківського працівника до вчинення злочину»*. Розкрадання та супутні йому злочини, що вчиняються безпосередньо в банках або з їх використанням, у переважній більшості неможливі без участі самих банкірів. Але, довести їх

причетність на практиці буває вкрай важко. Тому метою зазначеної тактичної операції є збирання доказів причетності працівників банку до вчинення злочину.

У рамках тактичної операції «Встановлення причетності працівників банку до злочину» проводяться наступні заходи:

- визначення кола працівників, які беруть участь у проведенні та оформленні конкретної банківської операції, а також організації контролю за її здійсненням;
- виявлення порушень порядку проведення та оформлення даної операції;
- визначення конкретних осіб, що зробили ці порушення;
- встановлення зв'язку працівників банку з іншими учасниками операції (працівниками банку та сторонніми особами).

Встановлення причетності працівника банку до вчинення злочину з використанням фінансової операції повинно починатися з вивчення необхідного нормативного матеріалу. Слідчий повинен чітко уявляти механізм здійснення банківської операції, особливості її відображення в первинних документах, облікових регістрах (у т.ч. данні електронного обігу), а також розподіл повноважень між працівниками, відповідальними за її проведення. Ця інформація міститься в нормативних актах Кабінету Міністрів України, Національного банку України. Більш докладно функціональні обов'язки працівників банку регламентуються у внутрішніх посадових інструкціях, що обов'язково мають бути у кожному банку.

Після ознайомлення із необхідними нормативно-правовими документами слідчий приступає до визначення кола осіб, що мають відношення до здійснення та оформлення відповідної банківської операції. Щоб визначити конкретних виконавців даної операції, необхідно вивчити всю документацію, пов'язану з її оформленням. Спочатку встановлюється персонал банку, який, згідно з інструкціями, повинен брати участь у здійсненні цієї операції, а потім проводиться перевірка наявності

необхідних повноважень в осіб, підписи яких фігурували в облікових документах. Іноді працівники банків у порушення відомчих інструкцій виконують окремі дії з оформлення та проведення банківських операцій, не володіючи для цього достатніми повноваженнями. Зустрічаються випадки, коли наприклад, економіст операційного відділу розписується від свого імені за інспектора-контролера даного відділу при видачі чи зарахуванні готівки, що категорично заборонено інструкціями банку. Це може свідчити про намір працівника банку на здійснення незаконних дій.

До призначення почеркознавчої та техніко-криміналістичної експертизи документів слідчий повинен упевнитися, чи ставили ці підписи зазначені у документі особи. Для цього необхідно під час допиту пред'явити працівникові банку підписані від його імені документи та запропонувати йому підтвердити дійсність підпису. У кожному випадку при виникненні сумнівів у дійсності підписів необхідно призначити почеркознавчу експертизу незалежно від того, чи підтвердив цей працівник факт підписання документа. Практиці відомі випадки, коли працівник банку, підозрюваний у здійсненні злочину, у судовому засіданні заперечував свої показання, надані в ході слідства щодо дійсності тих або інших реквізитів у документах.

Після встановлення кола осіб, що брали участь у проведенні та оформленні банківської операції, слідчий переходить до ретельного вивчення документів, вилучених у банку. Вони повинні досліджуватися на предмет їх наявності, змісту, правильності оформлення, відповідності іншим представленим документам.

Бажано на кожного учасника та виконавця документообігу заводити окремий «особовий рахунок», у який заносяться всі виявлені порушення. Наочне уявлення про механізм окремих злочинних дій у структурі технології незаконного збагачення, ймовірних учасників злочинної групи, розподіл ролей між співучасниками, характер нанесених збитків надає

можливість складання схеми руху цінностей із зазначенням всіх учасників операції.

Після того, як документальне оформлення операції перевірене повністю, необхідно проаналізувати наявну інформацію та спробувати виявити логіку порушень, наявність їх взаємозв'язку. Так, наприклад, при здійсненні дій з легалізації коштів, отриманих злочинним шляхом, банківські працівники здійснюють комплекс заходів, спрямованих на унеможливлення ідентифікації клієнта. Для цього при підготовці документів не вказуються номери договорів (або вказуються з помилками), відсутні у справі установчі документи підприємства чи організації, завуальована мета операції і та ін.

Аналізуючи виявлені порушення, слідчий може одержати інформацію, що свідчить про можливу причетність працівників банку до підготовки й вчинення злочину. Але, порушення можуть мати і ненавмисний характер. Сучасна банківська система не надто забезпечена кваліфікованими кадрами. Особливо це стосується так званих «фронт-офіс» працівників, які обслуговують клієнтів: операціоністи, економісти, інспектори з обслуговування клієнтів. Тому на сьогодні помилки в роботі, прорахунки, невимогливість керівництва до якості оформлення документів дуже поширені у банках.

Паралельно із цими заходами слідчий повинен установити наявність і характер зв'язків посадових осіб банку із клієнтами, які брали участь у здійсненні даної операції або в ній зацікавлені. Одержати подібну інформацію дуже важко. З цього приводу необхідне комплексне поєднання слідчих дій з використанням можливостей оперативно-розшукових заходів щодо спостереження за контактами представників банку, їх способом життя тощо. Часто про зв'язок працівника банку із клієнтами знають співробітники відділу, у якому він працює, члени його родини або друзі. Крім цього, слідчий може звернутися за допомогою до служб банківської безпеки, співробітники яких займаються забезпеченням охорони банку від

небажаного зовнішнього та внутрішнього впливу. Так чи інакше ця служба здійснює спостереження за працівниками банку, їх особистим життям, контактами, пересуванням. Таким чином, вони можуть володіти інформацією, що зацікавить слідство. Крім спостереження служба банківської безпеки має у своєму розпорядженні бази даних, які також можуть містити необхідні відомості. Володіючи такою інформацією, слідчий може обмежити коло підозрюваних, одержати додаткові докази вини банківського працівника.

Слідчий повинен враховувати специфіку добровільної участі працівників банку у вчиненні економічних злочинів, пов'язаних зі здійсненням банківських операцій. У цьому випадку недоцільно залучати осіб, підозрюваних у причетності до злочину, до проведення слідчих дій до моменту, коли всі необхідні докази його вини не будуть зібрані та проаналізовані. Найважливішу роль при проведенні розглянутої тактичної операції відіграє допит особи в якості підозрюваного (обвинувачуваного). При цьому необхідно забезпечити всебічну та ретельну підготовку до нього, у ході якої зібрати повну інформацію про причетність працівника банку до вчинення злочину.

Крім цього доцільно піддати перевірці інші операції, в оформленні або проведенні яких брав участь підозрюваний банківський працівник. Дослідження слідчо-судової практики показало, що в переважній більшості випадків (близько 65 % вивчених справ) банківські працівники, що добровільно брали участь у здійсненні розкрадань та інших корисливих злочинів, робили це неодноразово протягом тривалого періоду. За даними окремих досліджень, близько 35% посадових осіб банку, обвинувачених у зловживаннях брали участь у здійсненні подібних дій протягом усього строку роботи в банку. Тому доцільно перевіряти роботу відділу за тривалий строк (в ідеалі – від дня прийняття підозрюваного на роботу). Для скорочення обсягу роботи можна обмежитися операціями певного виду або операціями, проведеними за участю підозрюваного.

У результаті виявлення причетності працівників банку до вчинення злочинів у сфері економічної діяльності, ймовірна можливість одержання правдивих показань про основних суб'єктів злочинів, про існування організованої злочинної групи, а також про злочинну діяльність окремих банківських працівників і представників банківського керівництва.

ВИСНОВКИ

Дистанційне обслуговування клієнтів через мережу Інтернет, у т.ч. в банківській сфері, за останні роки значно покращили якість та швидкість взаємодії суб'єктів. Поряд з цим, телекомунікаційна мережа (кіберпростір) стала привабливою зоною для незаконного збагачення різного роду шахраїв та зловмисників. Корисливе злочинне втручання у роботу телекомунікаційних систем та мереж електронного зв'язку останнім часом набуває загрозливих масштабів, особливо в банківській сфері. Відсутність фізичного контакту з жертвою або представниками фінансової установи, а також анонімність, швидкість здійснення та невисокі витрати на здійснення злочину стали ключовими передумовами підвищення зацікавленості злочинців кіберпростором. Тому захист системи телекомунікацій типу «Клієнт-Банк» та своєчасне реагування правоохоронних органів щодо фактів несанкціонованого втручання у роботу системи ДБО клієнтів потребує постійного вдосконалення.

У роботі ми визначили, що факт незаконного втручання у роботу систем дистанційного банківського обслуговування має а меті чітко визначену корисливу складову – розкрадання коштів з рахунків клієнтів банку. І сам факт такого втручання є відповідним етапом на шляху злочинного збагачення. Технологія злочинної поведінки у даному випадку включає у себе, як правило, декілька осіб, які незаконно переводять грошові кошти з рахунків клієнтів банку на рахунки заздалегідь створених фіктивних фірм з подальшою їх конвертацією та легалізацією. Тому дії

злочинців підпадають під кваліфікацією за декількома статтями КК України. У складних злочинних схемах один злочин (підпорядкований) виступає необхідною умовою здійснення іншого, основного злочину, або ж є способом прикриття, маскування слідів кримінальних епізодів.

У рекомендаціях ми зазначили, що особливості кримінального провадження у по фактам несанкціонованого втручання в мережу ДБО і подальшого злочинного збагачення визначаються комплексним характером схем злочинної поведінки та змістом первинної інформації про злочин(и). Типові слідчі ситуації, які виникають на початковому етапі досудового слідства, розглянуті у рекомендаціях з урахуванням особливостей механізму злочинів; характеру вихідної інформації про злочин; за яким злочином (основним чи підпорядкованим) починається кримінальне провадження та результатами обізнаності слідчого про епізоди злочинної діяльності.

У ході кримінального провадження по даній категорії злочинів слідчому слід звернути увагу на розглянуті особливості тактики проведення окремих слідчих дій та тактичних операцій. Тактичні операції, у свою чергу, визначаються змістом завдань при конкретному кримінальному провадженні, а саме – а) встановлення обставин скоєння злочину, вилучення й фіксація його слідів, які можуть за тих чи інших обставин зникнути; б) встановлення, розшук і затримання особи, підозрюваної у вчиненні злочину; в) збирання доказів, достатніх для пред’явлення обвинувачення особі хоча б за одним епізодом злочинної діяльності.

Список рекомендованих та використаних джерел:

1. Аверьянова Т. В. Криминалистика: Учеб. для вузов / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская; под ред. Р. С. Белкина. – М.: Издат. группа НОРМА-ИНФРА-М,1999. – 992 с.
2. Волобуєв А.Ф. Розслідування і попередження розкрадань майна у сфері підприємництва: навчальний посібник / А.Ф. Волобуєв; [за ред. проф. О.М. Бандурки]. – Х.: Рубікон, 2000. – 272 с.
3. Журавель В.А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом: науково-практичний посібник / В.А. Журавель– Х.: ТОВ «Одіссей», 2005. – 312 с.
4. Особливості розслідування злочинів, вчинених шляхом кредитно-фінансових операцій : практичний посібник / В. В. Марков, В. В. Корнієнко. – Х. : НікаНова, 2012. - 65 с.
5. Лысенко В.В. Фиктивные фирмы (криминалистический анализ) / В.В. Лысенко. – К.: Парламентское изд-во, 2002. – 112 с.
6. Розгляд справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку // Офіційний портал Верховного Суду України / В.В. Антощук, М.І. Грицевим / Розділ: Судова практика. [Електронний ресурс]. – Режим доступу: http:// www.scourt.gov.ua/clients/vs.nsf/0/C8EABE11C12BFF3AC22576EE004F1E65 ?OpenDocument (10.01.2015)
7. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: автореф. дис. на здобуття наук. ступеня канд. юрид. наук за спец. 12.00.09 «кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / Тетяна Анатоліївна Пазинич; Харківський нац. ун-т внутр. справ. – Х., 2006. — 21 с.

8. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III // Відомості Верховної Ради України. – 2001. - № 5-6, ст.30.

9. Про затвердження Інструкції про безготівкові розрахунки в Україні в національній валюті: Постанова Національного банку України від 21.01.2004 року, № 22 // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0377-04

10. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень: Наказ Міністерства Юстиції України № 1950/5 від 26.12.2012 р. [Електронний ресурс] // Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0001-13/conv/print1354497610454545.

11. Протидія економічній злочинності / П.І. Орлов, А.Ф. Волобуєв, І.М. Осика, Р.Л. Степанюк, І.М. Зарецька, Е. Картер, Р. Ворнер. – Харків: Нац. ун-т внутр. справ, 2004. – 568 с.

12. Пчолкін В. Д. Теоретико-правові проблеми оперативно-розшукової діяльності: стан та напрями дослідження / В.Д. Пчолкін // Криміналістика XXI століття: Матеріали міжнародної науково-практичної конференції, 25-26 листопада 2010 р. – Х. : Право, 2010. – 832 с. С. 460-464.

13. Чернявський С. С. Злочини у сфері банківського кредитування (проблеми розслідування та попередження) : Навч. посібник / С. С. Чернявський; за заг.ред. О. М. Джужи. – К. : Юрінком Інтер, 2003. – 264 с.