14. *Логінова С. М.* Адвокатська таємниця: теорія і практика : автореф. дис.. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 / С. М. Логінова. – К., 2002.

15. *Обрізан Н.* Адвокатська таємниця у кримінальному процесі / Н. Обрізан // Підприємництво, господарство і право. – 2005. – № 6. – С. 144-147.

16. *Яновська О. Г.* Адвокатура України : навч. посіб. / О. Г. Яновська. – К. : Юрінком Інтер, 2007. – 280 с.

Погорецкий Н.Н. Понятие криминальных процессуальных гарантий адвокатской тайны. На основании анализа понятия уголовных процессуальных гарантий и понятия адвокатской тайны дано определение понятия уголовных процессуальных гарантий адвокатской тайны.

Ключевые слова: *адвокат, уголовные процессуальные гарантии, адвокатская тайна.*

Pohoretskyy M.M. Concept of criminal procedural guarantees of confidentiality. The article is based on the analysis of the concept of criminal procedural guarantees and the concept of confidentiality given to the definition of criminal procedural guarantees of confidentiality.

Based on the isolation and analysis of the essential features of criminal procedural safeguards, criminal procedural safeguards as defined by the criminal procedural law means and methods to achieve goals and objectives of the criminal justice system.

Criminal procedural guarantees of confidentiality are defined by the criminal procedural law means and methods of non-disclosure of any information that has become a prominent lawyer, paralegal, trainee lawyer, a person who is employed by an attorney, the client, as well as issues on which the client (a person who has refused to conclude a contract for assistance under this Act with reason) turned to a lawyer, law offices, law firms, content tips, advice, counsel for clarification, he composed documents, information stored on electronic media, and other documents and information received by a lawyer in the course of legal practice and the fact of client to an attorney for legal assistance in criminal proceedings.

Keywords: *attorney, criminal procedural guarantees of confidentiality.*

Надійшла до редакції 23.12.2013

Поїзд В.П.
начальник відділу
(Міністерство доходів і зборів України)

УДК 343.985

ОПЕРАТИВНО-РОЗШУКОВА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ, ВЧИНЕНИХ ЗА ДОПОМОГОЮ ВИСОКИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Здійснено аналітичний огляд наукових досліджень та практики протидії злочинам у сфері господарської діяльності, вчинених за допомогою високих інформаційних технологій, що надало можливість автору, з позиції фазового підходу, виділити чотири типові фази такої злочинної діяльності. Проаналізовано способи реалізації найбільш типових форм злочинної діяльності у сфері господарювання з використанням високих інформаційних технологій, а саме шахрайство у мережі Інтернет та незаконні дії з платіжними картками.

Ключові слова: *оперативно-розшукова характеристика, злочини у сфері господарської діяльності, високі інформаційні технології, шахрайство, платіжні картки.*

Постановка проблеми. Під час дослідження злочинності як соціального явища чи з позиції праксеології та вироблення оптимальних дієвих засобів впливу на неї, у тому числі й за допомогою негласних сил і засобів, особливої актуальності набуває глибинне з'ясування її сутності та специфічних ознак. Практика роботи оперативних підрозділів органів внутрішніх справ та податкової міліції свідчить, що у переважній більшості випадків ефективний алгоритм діяльності щодо виявлення, документування та розслідування конкретних фактів злочинної діяльності залежить від всебічного знання обстановки вчинення злочинів, типових способів (технологій) злочинної діяльності, класифікації та знання соціально-психологічних властивостей осіб, які становлять оперативний інтерес. Більш того, така інформація досить часто має стратегічний характер і дозволяє забезпечити ефективне оперативне обслуговування об'єктів та ліній роботи, якісно підбирати та розставляти негласний апарат, формуючи потужні агентурні мережі. Саме тому розроблення пропозицій щодо вдосконалення організації і тактики протидії злочинам у сфері господарської діяльності, які вчиняються за допомогою високих інформаційних технологій, потребує визначення їх оперативно-розшукової характеристики.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Мета. Останнім часом питання оперативно-розшукової характеристики злочинів досліджувалися К.В. Антоновим, С.В. Албулом, В.Д. Берназом, В.І. Василинчуком, О.Ф. Долженковим, В.В. Лисенком, Д.Й. Никифорчуком, В.А. Некрасовим, О.О. Подобним та іншими науковцями. Водночас проблематика оперативно-розшукової характеристики злочинів у сфері господарської діяльності, які вчиняються за допомогою високих інформаційних технологій, залишається недостатньо дослідженою.

Виклад основного матеріалу. Звертаючись до наукових здобутків криміналістичної науки, можна підтримати позицію професора В.В. Лисенка, що нині існує два основних підходи до побудови криміналістичної характеристики злочинів у сфері економіки: елементарний (побудований на описанні окремих елементів) та фазовий (описання фаз злочинної діяльності) [1, с. 73]. При цьому можна підтримати позицію С.Ю. Косарева, що цінність фазової моделі полягає у можливості простежити розвиток протиправної діяльності з моменту зародження злочинного умислу і сконструювати модель злочинної діяльності в її розвитку [2]. Більш того, окремі науковці-криміналісти пропонують замість аналізу криміналістичної характеристики злочинів вивчати структурно-функціональну модель злочинної діяльності, яка складається із таких елементів: мотив та цілі злочинного угруповання, його функціональна основа, програма злочинної діяльності з реалізації кримінального рішення, яка складається із самостійних стадій (інформаційно-пошукова стадія, організаційно-підготовча стадія, стадія виконання кримінального рішення і стадія із приховування злочинної діяльності угруповання) [3, с. 28-30]. Зазначимо, що у сучасній криміналістичній теорії фазовий підхід до аналізу злочинної діяльності призвів до появи нової наукової категорії «технологія злочинів», під якою розуміють функціонально зумовлену впорядковану сукупність дій (бездія-

льності), забезпечену відповідними ресурсами, що реалізується суб'єктами під час злочинної діяльності [4, с. 168].

На нашу думку, розглядаючи оперативно-розшукову характеристику злочинів цієї категорії, можна послугуватись викладеними методологічними здобутками криміналістики. Аналітичний огляд наукових досліджень свідчить, що у ході аналізу злочинної діяльності з позицій фазового підходу вчені виділяють такі типові чотири фази:

– збирання й оцінювання даних, на основі яких приймається рішення про можливість учинення злочину в конкретній ситуації;

– можлива зміна наявної ситуації, формування злочинної групи, коригування задуму, підготовка засобів;

– безпосередня реалізація злочинного наміру;

– розширення злочинних зв'язків і масштабів операцій, удосконалення засобів і технологій.

Переходячи до безпосереднього аналізу фазової моделі вчинення злочинів у сфері господарської діяльності із використанням високих інформаційних технологій, проаналізуємо конкретні етапи, які перебувають в інтенсивних залежностях між собою, водночас характеризуючись високим ступенем завершеності.

Вважаємо, що початковий етап злочинної діяльності може бути визначений як ***пошуково-аналітичний.*** Одразу зазначимо, що, відповідно до вивчених матеріалів практики роботи свідчих та оперативних підрозділів, на даній стадії у 72% випадків в особи сформовано стійку мотивацію та рішучість щодо вчинення злочинного діяння. Вивчення кримінальних проваджень та оперативно-розшукових справ свідчить, що на даному етапі злочинці діють як раціональні економічні агенти (відповідно до економічної теорії злочинності). Мається на увазі, що у більшості випадків аналітична робота, яка проводиться, зосереджена на аналізі таких факторів:

– оцінка прибутку, який планується отримати внаслідок вчинення злочину (злочинів);

– розрахунок супутніх витрат (освоєння спеціальних знань, придбання або виготовлення знарядь та засобів, у тому числі апаратних засобів та програмного забезпечення, розрахунок витрат на можливе встановлення корумпованих зв'язків та створення додаткових об'єктів у кіберпросторі тощо);

– аналіз витрат, пов'язаних із безпосереднім вчиненням злочину;

– аналіз можливих негативних наслідків вчинення злочину (затримання правоохоронними органами, засудження тощо) та вивчення можливості уникнення відповідальності за допомогою використання корумпованих зв'язків чи наявних фінансових активів.

При цьому необхідно звернути увагу, що у поведінці злочинців на цьому етапі спостерігається елемент «ірраціонального» мислення, оскільки вивчення кримінальних проваджень свідчить, що навіть якщо витрати на вчинення злочину перевищують потенційну вигоду, то 45,8% злочинців не відмовляються від реалізації злочинного задуму, а здійснюють пошук можливих шляхів оптимізації витрат.

Наступною складовою цієї стадії є вибір об'єкта злочинного посяган-

ня, що передбачає детальне вивчення інфраструктури його обслуговування. У зв'язку з тим, що сучасна інформаційно-телекомунікаційна інфраструктура є досить складною, для аналізу та вивчення об'єкта злочинного посягання, як правило, залучається спеціаліст у сфері високих інформаційних технологій. Вивчення оперативно-розшукових справ свідчить, що існує декілька типових способів залучення фахівця на даній стадії:

– фахівець у сфері високих інформаційних технологій, надаючи консультативні послуги, не знає, що бере участь у підготовці до вчинення злочинів. У таких випадках особа-консультант досить часто виконує «дружню» послугу знайомому, не вдаючись у мотивацію його поведінки. Крім того, у практиці роботи правоохоронних органів трапляються випадки, коли до аналізу потенційного об'єкта кримінального посягання залучаються неповнолітні, які мають кваліфіковану самопідготовку у сфері високих інформаційних технологій. Зазначимо, що такий спосіб залучення фахівця не завжди забезпечує беззаперечне досягнення злочинного результату, оскільки, не знаючи про мету аналізу, останній досить часто проводиться поверхнево;

– фахівець у сфері високих інформаційних технологій, надаючи консультаційні послуги, знає, що бере участь у підготовці злочину. Такий спосіб є результативнішим з позиції досягнення злочинного результату. Як свідчить вивчення матеріалів практики, такі фахівці проводять досить детальне вивчення об'єкта злочинного посягання. Також спостерігається зміна методів роботи аналітиків кримінальних угруповань та освоєння інноваційних концепцій роботи з інформацією, наприклад використання великих масивів даних, що передбачає стовідсотковий аналіз усієї наявної інформації стосовно об'єкта з використанням заздалегідь написаних програмних продуктів та алгоритмів.

Вивчення матеріалів практики та спеціалізованих видань свідчить, що пошук потенційного об'єкта злочинного посягання відбувається скануванням мережі Інтернет за допомогою спеціалізованого програмного забезпечення. При цьому, як свідчить опитування працівників оперативних підрозділів, у 92% випадків виявити підготовчі дії щодо вчинення злочину за допомогою технічних засобів фактично неможливо, і тому у даному випадку ефективним є проведення традиційних оперативно-розшукових заходів.

У типовий набір фахівця у сфері високих інформаційних технологій, використовуваний під час вивчення об'єкта злочинного посягання, входять: сканери телефонних ліній; зламувачі та генератори паролів, засоби шифрування, а також цілі програмні пакети, які комплексно автоматизують операції зламів (наприклад, CiberKit). Традиційно злочинцями для визначення апаратних засобів, які мають модемний вхід, використовується спеціалізоване програмне забезпечення (PhoneSweep, Tolenoc), яке поступово встановлює зв'язок з телефонними номерами, що знаходяться у відповідному діапазоні. Номери, на які відкликається модем, реєструються у відповідному файлі (аналогічні методи використовуються для виявлення уразливих місць комп'ютерів, підключених до Інтернету). Досить часто з цією метою використовуються стандартні програми пошуку вразливості мережі і сканувальні програми, які поступово підбирають усі можливі точки доступу до систе-

ми з метою визначення найоптимальнішого варіанта проникнення.

Серед найпоширеніших інструментів необхідно також виділити сканери портів комп'ютера, які в автоматичному режимі запитують кожен порт комп'ютера, з'ясовуючи, який з них є відкритим. У даному випадку комп'ютер автоматично відправляє звіт, надаючи необхідну для аналізу інформацію. Таке «зондування» портів дозволяє виявити найвразливіші з них для атак.

Аналіз спеціалізованої комп'ютерної літератури свідчить про наявність значної кількості програм-сканерів, які характеризуються різними алгоритмами роботи та функціональним призначенням. Так, один з найрозвинутіших пакетів CyberCorp Scanner має можливість перевірки і оцінки уразливості локальних корпоративних мереж, розширений набір додаткових інструментів для моніторингу ефективних вторгнень, може перевіряти робочі станції і сервери, має концентратори, комутатори і включає спеціалізовані трасувальники пакетів для перевірки маршрутизаторів.

Традиційно на цьому підготовчому етапі злочинці намагаються отримати доступ до системних паролів перехопленням, підбиранням з використанням програмних засобів або за допомогою типової крадіжки фізичних носіїв з даними. Поширеними у перехопленні залишаються програмні засоби типу «сниффер», які вбудовуються у чужі комп'ютери або системи та дозволяють здійснювати моніторинг й аналіз системи протягом тривалого часу без явних ознак злочинної діяльності.

Наступним етапом є ***формування групи та підготовка засобів.*** У ході аналізу цього етапу на особливу увагу заслуговує методика втягнення у злочинну діяльність персоналу установ чи організацій, де планується вчинення злочину. Вивчення кримінальних проваджень свідчить, що залучення персоналу до злочинної діяльності відбувається з використанням:

– погроз (застосування фізичного насильства, оприлюднення компрометуючих матеріалів тощо);

– підкупу (традиційно використовується стосовно працівників професійної ланки, які мають відповідний доступ, а також осіб, які мають фінансові проблеми);

– інші чинники (інтимні стосунки зі злочинцем, помста керівництву, самоствердження тощо).

Вивчення практичних матеріалів свідчить, що пріоритетними об'єктами для встановлення злочинних зв'язків з персоналом сьогодні є: фінансові структури; провайдери доступу; електронні магазини; міжнародні корпорації; сайти неурядових фінансових організацій.

Вважаємо, що способи сприяння персоналу установи (організації) злочинцям можна згрупувати у три блоки:

– умисне невжиття заходів щодо збереження паролів, іншої конфіденційної інформації та розголошення відомостей щодо конфіденційної інформації, яка знаходиться у мережі;

– невиконання належних заходів захисту, зокрема допуск до роботи у локальних мережах сторонніх осіб;

– неповідомлення керівництву чи правоохоронним органам про виявлені ознаки злочинної активності у мережі.

Безперечно, що основним етапом є ***безпосередня реалізація злочинного задуму***. Зважаючи на те, що спектр розглядуваних діянь є досить широким, проаналізуємо способи реалізації найбільш типових форм злочинної діяльності у сфері господарювання з використанням високих інформаційних технологій.

1. Шахрайства у мережі Інтернет. Поширення шахрайств у мережі Інтернет насамперед пов'язано із появою електронних магазинів, особливості функціонування яких і приваблюють злочинців. Так, витративши невелику суму на створення Інтернет-магазину, можна імітувати нормальну торговельну діяльність із подальшим вчиненням шахрайських дій щодо споживачів. Як свідчить аналіз практики роботи органів податкової міліції та оперативних підрозділів ДСБЕЗ, окрім використання фіктивних Інтернет-магазинів, злочинці застосовують широкий спектр обманних способів заволодіння грошовими коштами, зокрема:

– псевдосайти благодійних, релігійних організацій тощо, які збирають пожертви;

– спам-розсилання і сайти з проханнями про матеріальну допомогу для лікування тощо;

– сайти фіктивних шлюбних агенцій і окремі віртуальні наречені;

– шахрайські он-лайн банки та інвестиційні фонди, які обіцяють значні відсотки за вкладами;

– розсилання та сайти з повідомленнями інформації про виявлені уразливі місця у платіжних системах, які дозволяють примножити свій прибуток після переказу певної суми коштів на рахунок злочинців;

– шахрайські сайти і розсилання, які пропонують віддалену роботу, з перерахуванням початкового вкладу.

Усі зазначені способи мають спільний типовий алгоритм дій злочинців: розміщення інформації в Інтернеті – встановлення анонімного контакту з потерпілим – отримання від нього коштів – зникнення з мережі та поява в подальшому за новою IP-адресою.

Поряд із типовими способами вчинення цього злочину необхідно проаналізувати окремі особливості Інтернет-магазинів, які свідчать про їх створення з метою вчинення злочинів, що дозволить значно покращити оперативне обслуговування національного сегменту мережі Інтернет з боку працівників оперативних підрозділів. Так, у результаті вивчення оперативно-розшукових справ та опитування працівників оперативних підрозділів виділено окремі блоки відомостей, які свідчать про можливу злочинну мету створення Інтернет-магазину:

– явна економія на утриманні сайту, рекламі, персоналі, послугах зв'язку тощо (у даному випадку злочинці не створюють повноцінний магазин, а обмежуються лише «фасадом», дизайн сайту та товарний знак є часто запозиченими, замовлення обробляються в ручному режимі, не використовуються банківські рахунки);

– намагання приховати особу власника там, де вона має вказуватися (під час реєстрації доменного імені, придбання послуг зв'язку, розміщення реклами тощо);

– використання виключно таких способів оплати, які дозволяють приховати дані власника, неможливість оплати кур'єру під час отримання товару;

– період між замовленням товару та його доставкою є максимально великим;

– відсутні товари економ-класу.

2. Незаконні дії з платіжними картками. Практика роботи оперативних підрозділів свідчить про наявність декількох способів незаконних дій з платіжними картками. Водночас для усіх з них характерними є три типові фази вчинення злочину:

– отримання даних щодо платіжних карток різноманітними способами;

– сортування, класифікація та їх реалізація як іншим кримінальним угрупованням;

– безпосередня конвертація коштів, які знаходяться на банківській картці, у готівку.

При цьому складність технологічного процесу вчинення таких злочинних дій зумовлює їх скоєння завжди групою осіб, оскільки кожна із стадій пов'язана із необхідністю наявності спеціальних знань, досвіду у відповідній сфері, посадовим становищем, доступом до апаратних засобів та програмного забезпечення.

Для вироблення ефективного алгоритму протидії злочинам означеної категорії слушно визначити на основі вивчення матеріалів кримінальних проваджень та оперативно-розшукових справ типові способи незаконного отримання даних стосовно пластикових платіжних карток, а саме:

– дистанційний неправомірний доступ до серверу, де зберігаються чи обробляються такі дані, наприклад сервер магазину чи банку (досить рідко зустрічається на практиці – 13% випадків);

– доступ до даних з використанням свого посадового становища і недоліків у системі захисту підприємства (спосіб є поширеним, оскільки власники підприємств часто звертають підвищену увагу на захист від зовнішніх загроз, нехтуючи внутрішньою інформаційною безпекою підприємства);

– перехоплення трафіку у випадку, коли дані картки передаються у відкритому доступі (вказаний спосіб перебуває у прямому взаємозв'язку з віктимною поведінкою потерпілого);

– отримання даних банківських карток або знання дампу під час обслуговування клієнтів у закладах торгівлі і харчування (необхідний безпосередньо фізичний контакт з картою);

– виманювання даних та пін-кодів за допомогою заходів фішшингу;

– фізичне заволодіння картою через обман потерпілого.

Складнішими є способи безпосереднього отримання готівки з банківських платіжних карток. До найпоширеніших з них можна віднести такі:

– речовий кардинг – придбання в Інтернет-магазинах або у реальних (фізичних) торговельних точках товарів з метою власного використання, на замовлення, з метою перепродажу;

– здійснення фіктивних придбань в Інтернет-магазинах чи придбання послуг платних сайтів за попередньою домовленістю з їх власниками (за допомогою карти здійснюється оплата, після чого частина коштів поверта-

ється злочинцю власником сайту);

– гра в Інтернет-казино (заздалегідь найняті особи реєструють в Інтернет-казино багато аккаунтів на ім'я власника карти, вносять депозит з карти та розпочинають гру, а в подальшому виводять виграш на інші рахунки).

Аналізуючи діяльність Інтернет-казино, необхідно звернути увагу на окремі аспекти, які ускладнюють використання цього способу злочинної діяльності на сучасному етапі. Досить часто для виплати коштів казино вимагає підтвердження особи гравця, а також не використовує анонімні системи платежів. Від гравця, який хоче отримати виграш, можуть вимагати вислати скан-копію паспорта та документа, який підтверджує фактичне місце проживання. В окремих випадках, як свідчить практика, від гравця вимагають номер телефону для підтвердження його особи. Виплата у подальшому здійснюється на іменний банківський рахунок або за допомогою іменного чеку, який відправляється поштою.

Водночас, перебуваючи у постійній боротьбі, способи протидії злочинній діяльності змусили модифікуватись останню. Сьогодні у мережі можна знайти послугу з виготовлення точних копій скан-паспортів та інших документів, телефонні номери у «благонадійних» країнах із переведенням дзвінків у будь-яку частину світу, банківські рахунки, на які приймають кошти, адресовані будь-яким фізичним особам тощо;

– використання інших Інтернет-сервісів, де можливим є отримання коштів, наприклад перегляд любительського кіно;

– зняття готівки у банкоматах у випадку наявності пін-коду (виготовляється тверда копія картки – «білий пластик», з якої знімається максимально доступна сума за максимально короткий проміжок часу).

Висновок. Вважаємо, що на окремий аналіз заслуговує характеристика криміногенного потенціалу платежів, які здійснюються через мережу Інтернет. Сьогодні поряд з банківськими платіжними системами та методами, які врегульовані як внутрішнім законодавством України, так і міжнародно-правовими актами, існує значна кількість платіжних систем, які не є банківськими і не контролюються належним чином з боку державних органів. Не зупиняючись на детальній характеристиці змісту функціонування вказаних систем, зазначимо, що усі вони пов'язані відповідною системою посередників, які дають можливість швидко конвертувати кошти та переводити їх з однієї системи до іншої, ускладнюючи тим самим відстеження та блокування кримінальних трансакцій. Крім того, з аналізу правоохоронної практики можна дійти висновку, що існує і система вторинних послуг – управління рахунками платіжних систем, введення та виведення коштів, у тому числі й анонімно.

Значна кількість мережевих платіжних систем емітують, співпрацюючи з банками, свої власні пластикові картки, за допомогою яких можна переказувати кошти з подальшим зняттям у будь-якому банкоматі. Для випуску такої карти необхідно надати паспорт або його скан-копію, але перевірка особи, як правило, здійснюється формально, що дозволяє безперешкодно отримати картку на чуже ім'я. Більш того, сьогодні можна з упевненістю говорити про появу ринку таких карток, які вільно продаються у

мережі. Така опція надає злочинцям можливість використовувати рахунок «WebMoney» чи «E-gold» для отримання кримінальних платежів, наприклад прибутків від кардерської діяльності. У даному випадку зарахована у «гаманець» сума швидко переводиться через декілька рахунків на картковий рахунок, при цьому використовується веб-інтерфейс управління рахунком, який забезпечує анонімність користувача.

Бібліографічні посилання

1. *Лисенко В. В.* Криміналістичне забезпечення діяльності податкової міліції: теорія і практика : монографія / Лисенко В. В. – К. : ЛОГОС, 2004. – 210 с.

2. *Косарев С. Ю.* Криминалистические методики расследования преступлений: генезис, современное состояние и перспективы развития : дис. … докт. юрид. наук / С.Ю. Косарев. – СПб., 2005.

3. *Отряхин В. И.* Методика расследования хищений в сфере банковской деятельности : дис. … канд. юрид. наук / В.И. Отряхин. – М., 2001.

4. *Шмонин А. В.* Методология криминалистической методики : монография / Шмонин А. В. – М. : Юрлитинформ, 2010.

Поезд В.П. Оперативно-розыскная характеристика преступлений в сфере хозяйственной деятельности, совершенных при помощи високих информационных технологий. Осуществлен аналитический обзор научных исследований и практики противодействия преступлениям в сфере хозяйственной деятельности, совершенных с помощью высоких информационных технологий, что сделало возможным, с позиции фазового подхода, выделить четыре типичные фазы такой преступной деятельности. Проанализированы способы реализации наиболее типичных форм преступной деятельности в сфере хозяйствования, с использованием высоких информационных технологий, а именно мошенничество в сети Интернет и незаконные действия с платежными карточками.

Ключевые слова: *оперативно-розыскная характеристика, преступления в сфере хозяйственной деятельности, высокие информационные технологии, мошенничество, платежные карточки.*

Poyizd V.P. Operational-search description of economic crimes committed with the use of high IT. The article presents an analytical review of research and practice of combating crimes in the field of economics committed by means of information technologies that has enabled the author, based on professional approach, to define four standard stages of such criminal activity. The practice of operational departments of the police and the tax police shows that in most cases, an efficient algorithm in identifying, documentation and investigation of specific cases of criminal activity depends on thorough research of the situation in which a crime is commited, typical methods (technology) of criminal activity, classification and knowledge of social and psychological characteristics of persons who are in the operational interest. Furthermore, such information is often strategic and allows to provide an efficient operational services of objects and lines of work, efficiently choose and deploy secret surveillance by forming the powerful agent networks. That is why the development of proposals for improving the organization and tactics of combating crimes in the field of economics committed by means of information technologies requires the definition of their operational characteristics. The ways of realization of the most common criminal activities in economics with the use of information technology, such as Internet fraud and illegal actions with payment cards are analysed. According to the author, a special analysis should be devoted to the characteristics of criminal potential of payments that are made through the Internet. Nowadays, alongside with bank payment systems and methods that are regulated by the internal legislation of Ukraine as well as international regulations, there are a number of payment systems that are not bank payment systems and are not controlled properly by the public authorities.

Keywords: *operational-search description, crimes committed in the field of economics, high IT, fraud, payment cards.*

Надійшла до редакції 24.12.2013