УДК 343.98.06 : 343.451

О. В. КАЛИНОВСЬКИЙ
Р. О. БОЛГОВ

ЗАСТОСУВАННЯ КЛАСИЧНИХ МЕТОДІВ КРИМІНАЛІСТИКИ ТА СУЧАСНИХ ТЕХНОЛОГІЧНИХ МОЖЛИВОСТЕЙ У ПРИВАТНІЙ ДЕТЕКТИВНІЙ ПРАКТИЦІ ПРИ РОЗСЛІДУВАННІ КІБЕРШАХРАЙСТВА

Розвиток сучасних технологій дав поштовх для виникнення злочинів нового покоління — кіберзлочинів. До кіберзлочинів належать, в тому числі, і шахрайство в Інтернеті («нігерійські» листи, афери з банківськими картами, збір коштів для допомоги дітям з завідомо неправдивими фотографіями тощо). За якими ознаками можна розпізнати інтернет-шахрая? Як передати його в руки правосуддя? Які механізми протидії та запобігання таких злочинів? У статті наведено приклади викриття деяких кібершахрайських схем як за допомогою класичних методів криміналістики так і з використанням сучасних технологічних можливостей. Висвітлено унікальний досвід досудового розслідування з залученням приватних детективів, співробітників Департаменту кіберполіції Національної поліції України та журналістів.

Ключові слова: *кіберзлочин, інтернет-шахрайство, кібершахрайство приватний детектив, кіберполіція, досудове розслідування.*

Kalinovsky Alexander, Bolgov Ruslan. **Application of classical criminalistic methods and modern technological opportunities in the private detective practice at investigation of kibershage**

The development of modern technology has given impetus to the emergence of crimes of a new generation — cybercrime. The most common types of cybercrime include various types of online fraud («Nigerian» letters, bank card fraud, fundraising for children with knowingly false photographs, etc.). By what signs can you recognize the internet scam? How to put it in the hands of justice? What are the mechanisms for preventing and combating such crimes? The article presents examples of the disclosure of some cybercrime schemes, both with the help of classical methods of forensics, and with the use of modern technological possibilities.

© *КАЛИНОВСЬКИЙ Олександр Валерійович* — кандидат юридичних наук, старший науковий співробітник Національної академії внутрішніх справ

© *БОЛГОВ Руслан Олегович* — аспірант Національної академії внутрішніх справ, приватний детектив

The unique experience of interaction of private detectives, employees of the Department of Cyberpolicies and journalists during the pre-trial investigation is shown.

Key words: *cybercrime, internet fraud, cybercrime, private detective, cyberpolice, pre-trial investigation.*

У сучасних умовах шахрайство набуває дедалі більшого розповсюдження та різноманітності, і тому проблема захисту майна від таких посягань не втрачає свою актуальність. Варто зазначити, що проблема захисту від таких злодіянь потребують не тільки громадяни, а і банківська сфера. Ст. 190 Кримінального Кодексу України (КК України) визначає шахрайство як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, внаслідок чого, фізичні та (або) юридичні особи позбавляються матеріальних цінностей, можливості користуватися майном яке їм належить, відповідно до його цільового призначення[1]. Офіційна статистика України свідчить, що протягом 2017 року було зареєстровано 36650 злочинів за ст. 190 (шахрайство), з яких тільки в 10147 випадках вручено повідомлення про підозру, а 26503 злочинів так і залишилися не розкритими. Однак при порівнянні звітного періоду за січень-березень 2017 р. (14699 по ст. 190) з періодом за січень-березень 2018 р. (10868 по ст.190) можна відзначити істотне зниження рівня вчинення даного виду злочинів[2]. Такі статистичні дані можуть свідчити, з одного боку, на зниження кількості зареєстрованих кримінальних правопорушень, а з іншого — до зниження кількості звернень громадян до правоохоронних органів за цією статтею у зв'язку з низькою ймовірністю повернення втраченого. Це підтверджує положення, що вчасне виявлення різних схем шахрайств і розголошення їх широкій аудиторії з метою запобіганню їх вчинення, дає можливість запобігти подібним кримінальним правопорушенням.

Кінець XX ст. ознаменувався стрімким розвитком інформаційних технологій, що почали впроваджуватися в усі сфери життєдіяльності. Використання сучасних персональних комп'ютерів, інформаційно-обчислюваних мереж забезпечило

кожній особі можливість доступу до інформації, що зберігається у відповідних базах даних незалежно від доби і місцезнаходження абонента. Поряд з перевагами, розвиток інформаційних технологій призвів і до негативних наслідків, серед яких — поява нового виду злочинності — кіберзлочинності. До кіберзлочинів відносять всі типи кримінальної активності, що здійснюються з використанням гаджетів та комп'ютерів та/або Інтернету. Поняття «кіберзлочинність» часто вживається поряд з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». На сьогодні, найбільш розповсюдженим є умовний поділ кіберзлочинів на: агресивні та неагресивні. До першої групи належать: кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає кіберкрадіжку, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм[3].

Кримінальний кодекс України (розділ XVI) оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених поняття «кіберзлочинність» є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство[4].

Відомо, що зібрання доказової бази при досудовому розслідуванні шахрайства є досить непростим[5], а виявлення і встановлення доказів кібершахрайства — ще складніша задача. Варто зазначити, що «злочинці нового покоління» так само використовують і старі методи в симбіозі з новими можливостями системних інновацій.

Об'єктом дослідження є: пости, які містять завідомо неправдиву інформацію (в соціальних мережах і месендже-

рах, смс-повідомленнях), які розміщувалися з метою заволодіння грошовою сумою шляхом зловживання довірою, та «листи щастя» або так звані «нігерійські листи» — давній спосіб шахрайства в системі Інтернет. Співробітники Департаменту кіберполіції Національної поліції України активно працюють над виявленням та розкриттям різних схем кібершахрайства[6] і практика показує, що звернення до кіберполіції є першим і важливим кроком у протидії таким кримінальним правопорушенням.

Так, у травні 2016 р. у мережі Facebook з'явився пост користувача, в якому оприлюднювалися світлини дівчинки з явними опіками шкіри (на фото була зображена дитина з опіками майже по всьому тілу на лікарняному ліжку) та прохання на збір коштів для її лікування. Автор посту позиціонувала себе як мама дівчинки яка благала про допомогу для своєї доньки, що нібито впала у відро з окропом. До даного посту були прикріплені фото дитини з лікарні з великими опіками. Подібні пости не є поодинокими в мережі інтернет, вони висвітлюють певну трагічну історію і спонукають до переведення коштів на зазначені у постах рахунки або хоча б репосту. Однак, дані з цього посту вказували на те, що цей пост є ні що інше як яскравий приклад кібершахрайства –зловживання довірою особи з метою заволодіння майном (в даному випадку, грошима). Для доведення того, що згадана публікація містить ознаки кібершахрайства, приватними детективами був проведений моніторинг всесвітньої мережі в пошуках зазначеного фото на збіг, за результатом якого він був знайдений. Як з'ясувалося, дитина на фото в окріп не падала, а отримала такі великі опіки під час пожежі 11 років тому у травні 2007 р.[7]

Після проведеної нами ретельної перевірки було виявлено, що дану публікацію у Facebook використовували ще кілька людей. Отримані в ході цього аналізу постів дані були передані офіційною заявою через сайт кіберполіції. На підставі заяви та поданих матеріалів, було відкрито кримінальне провадження за ч. 3 ст. 190 КК України (шахрайство) відносно осіб, які були власниками банківських карт і знімали кошти з зазначених

карток. Наразі, усі особи встановлені, проводиться досудове розслідування.

Як відомо, методи криміналістики відіграють важливу роль при розслідуванні злочинів. Серед класичних методів криміналістики, які широко використовуються у детективній практиці під час виявлення ознак обману, шахрайства або інших маніпуляцій, важливе місце посідають логічні (аналіз, синтез, індукція, дедукція, гіпотеза, аналогія, ідеалізація узагальнення) та почуттєво раціональні (спостереження, опис, порівняння)[8]. Порівняння — це один з універсальних методів наукового пізнання, що дозволяє встановлювати схожість і відмінність предметів, які досліджуюсь та явищ реальної дійсності. За допомогою порівняння виявляються якісні та кількісні характеристики досліджуваних об'єктів, класифікується, упорядковується і оцінюється зміст буття і пізнання. Порівняти - означає зіставити одне з іншим з метою виявлення їх співвідношення. Оскільки порівняння має на меті виявлення того загального або різного, що є у порівнюваних об'єктів[9].

У ході досудового розслідування цих злочинів, було встановлено ще кілька осіб, які використовували ці пости з метою отримання коштів. Так, в тому ж 2016 р., приватними детективами був виявлений пост у Facebook, автори якого збирали кошти для нібито допомоги дівчині хворій на рак, яка знаходилася в одній з лікарень м. Києва. У пості були вказані дані дівчинки і її мами, їх контактні телефони та реквізити банківських карт. Були прикріплені світлини дівчинки без волосся на лікарняному ліжку і фото, де вона з волоссям і нібито так само у лікарні з сумним виглядом.

Першочергові методи перевірки не дали змоги одразу з'ясувати справжність даного посту або довести, що це підробка для шахрайських дій. Тому, для подальшої перевірки, були використані всі можливості криміналістичного порівняльного аналізу і сучасних можливостей в технологічній сфері.

Увагу привернуло саме фото, де дівчина була із волоссям і з сумним виглядом. Фото відрізнялося від інших і не була схожа на фото з лікарні. На даному фото були зображені повітряна

кулька з нечітким надписом, кілька телевізорів на задньому плані в нестандартних кольорових рамках та покривало, яке знімали з дівчинки. Є безліч надписів на кульках, але вони в основному всі стандартні. Ми припустили, що форма надпису та малюнок на повітряній кульці зроблені за індивідуальним замовленням. На жаль, надпис прочитати не вдалося через низьку якість фотографії, але цей маленький факт дав поштовх для пошуків в цьому напрямку. Використовуючи один з найдавніших логічних методів криміналістики — індукцію — та пошукові можливості всесвітньої павутини, було зроблено висновок, що світлина було зроблена не в лікарні, а в перукарні, до того ж дитячій. Так почався пошук за ключовими словами в Інтернеті, в результаті був знайдено довгоочікувану кульку з чітким надписом та з назвою перукарні. Як з'ясувалося, це була мережа дитячих перукарень Росії, зокрема, в Санкт-Петербурзі.

Шляхом порівняльного аналізу наданих світлин з сайту перукарні з світлинами з шахрайського посту було встановлено адресу, де була зроблена шукана світлина та контакти адміністратора даного закладу. Внаслідок чого, нам вдалося з'ясувати хто був зображений на фото, як виявилося, ця дівчинка була постійним клієнтом перукарні і не страждала на ті хвороби, про які йшлося в шахрайському пості. Більше того, в Україні вона ніколи не була. Тобто ми з'ясували, що це були фото різних дівчат. Дана інформація не привела нас до імені справжньої дівчинки з фото на лікарняному ліжку, але була доказом того, що її цілеспрямовано використовували з метою незаконного збагачення шляхом спланованого обману.

Паралельно з цим розслідуванням велися пошуки дівчини, чиї фото використовували шахраї в соцмережі Facebook. Пропустивши всі фотографії зі сторінки шахраїв, через пошукові можливості різних браузерів, було виявлено справжню власницю фотографій. При аналізі та порівнянні фотографій з двох сторінок, в цьому переконалися остаточно. Справжня власниця фото дала свідчення, що не має ніякого відношення до вищезазначеного профілю у соцмережі Facebook і це підтвердилося іншими слідчими (розшуковими) діями.

Також (зі спеціально створеного для розслідування акаунту) нами здійснювалося листування з особою, що розмістила шахрайський пост. Під час цього листування було згенеровано кілька посилань, які були вбудовані в код фотографії з чеком про грошовий переказ. Посилання дозволяло при натисканні на нього, визначити IP адресу з якого було натиснуте посилання а також — точний час, коли це було зроблено. Дані фото були відправлені особі, що розмістила шахрайський пост і нею було здійснено перехід за цим посиланням, щоб переконатися в переказі коштів. Це дало можливість встановити провайдера особи, яка знаходилась по той бік монітору і її місце знаходження.

В рамках кримінального провадження по даному факту, було офіційно отримано відомості про власників банківських карт, і прив'язаних до них номерів телефонів. Звісно, що картками користувалися не їх власники, вони були звичайними дропами, однак, телефони були реальні, оскільки без них складно проводити операції з картами.

З'ясувавши орієнтовне місце знаходження телефонів із отриманої інформації, за допомогою методу згенерований посилань, ми отримали один і той самий район місцезнаходження комп'ютера підозрюваної особи, з якою велося листування. Адреса була поруч з місцем проживання власника однієї з карт. Це наштовхнуло на думку про можливе тісне знайомство власника карти і того, у кого ця карта знаходилась. Маючи фото власника карти з банку та фото того, хто знімав кошти з банкомату (отриманої з камери спостереження банкомату), ми провели аналіз, який показав, що це різні люди. Після проведених обшуків (на законних підставах в рамках кримінального провадження,) в одній із записних книжок власника банківської карти було виявлено телефон, яким користувався шахрай.

Таким чином, у ході взаємодії приватного детектива та представників Департаменту кіберполіції Національної поліції України, класичні методи криміналістики і сучасні технології (згенеровані посилання, фото з камери спостереження банкомату та ін.), дали можливість виявити та процесуально закрі-

пити факти кібершахрайства, встановити підозрюваних осіб і розпочати кримінальне провадження. Наразі по кримінальним провадженням проводяться подальші слідчі дії.

На основі власного досвіду досудового розслідування таких кримінальних злочинів ми встановити які основні складові шахрайства в мережі *(рис. 1)*:

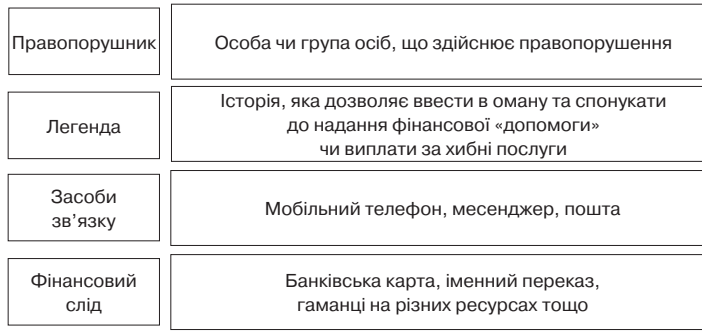

Рис. 1. Гіпотетичні складові кібершахрайства

Без цих складових шахрайство неможливе і саме ці складові і є «Ахіллесовою п'ятою» шахраїв. Саме ці складові у повному обсязі шахраї намагаються приховати, маніпулюючи свідомістю людей і спотворюючи інформацію.

Наступний спосіб кібершахрайства, якому стільки ж років скільки самому Інтернету і навіть більше — це листи щастя, або так звані «Нігерійські листи». Багато хто отримував такого листа, в якому на досить неграмотній мові (ймовірно, з використанням гугл-перекладача), йшлося нібито що вам про вам залишили спадок або ви настільки прекрасні, що офіцер США хоче одружитися з вами, або прекрасна незнайомка (самотня і заможна) хоче вийти заміж. Листи названі так тому, що особливе поширення цей вид шахрайства отримав в Нігерії ще до поширення Інтернету, коли такі листи поширювалися звичайною поштою. Одна з перших розсилок датована ще в 80-х роках. Однак сьогодні «Нігерійські листи» приходять і з інших африканських країн, а також з міст з великою

нігерійської діаспорою (Лондон, Амстердам, Мадрид, Дубай)[10].

Як правило, такі шахраї просять у одержувача листа допомоги в багатомільйонних грошових операціях, обіцяючи солідні відсотки із сум. Оскільки шахраям стало доступно набагато більше інформації про жертву через соціальні мережі, тепер вони вже звертаються особисто в месенджер до жертви і це викликає ще більшу довіру у людей, зокрема в тих, які звикли вірити в диво. Якщо одержувач погодиться брати участь, у нього поступово виманюються дедалі більші суми грошей, нібито, на оформлення угод, сплату зборів, хабарі чиновникам тощо. Але частіше це інформація про можливе отримання спадщини — а для його отримання потрібно оплатити послуги адвоката. Є і інша схема таких кібершахрайств — обман довірливих самотніх жінок і чоловіків, в яких, за допомогою привабливих та «солодких» обіцянок під час приватного листування, виманюють кошти. Вивчаючи таки схеми отримуємо криміналістично-значущу інформацію, а саме час, місце, спосіб та саме головне це суб'єктивну сторону, як визначає шахрайство та способи його вчинення. Суб'єктивна сторона шахрайства характеризується прямим умислом і корисливим мотивом. У вказаному ж випадку чітко бачимо опис класичного шахрайства, в якому використовують спосіб активного обману або зловживанням довірою, де чітко простежується корисливий мотив. Наразі необхідно зазначити, що шахрайство вважається закінченим лише з моменту переходу чужого майна у володіння винного або з моменту отримання ним права розпоряджатися таким майном. Це необхідно знати під час звернення до лав поліції із заявою про шахрайство, в противному випадку не буде складу злочину.

На сьогодні приватними детективами проведено кілька масштабних розслідувань разом з кіберполіцією та журналістами з приводу таких листів, викрито схеми маніпуляцій свідомістю людей, виявлені справжні люди, фото яких використовують в таких аферах, знайдені і висвітлені способи перевірки таких листів на причетність до шахрайських схем[11].

Ще одним видом кібершахрайства є різноманітні схеми заволодіння банківськими картками. Шахраї використовують дані потенційної жертви (як правило, це номер телефону з інтернет-оголошень про продаж майна або навіть дані з персональних сторінок у соцмережах) і, за допомогою «легенди», потенційна жертва власноруч просто робить основним фінансовим телефоном своєї банківської картки телефон картки шахрая. Внаслідок чого, жертва особисто передає права на доступ до своїх коштів через інтернет-банкінг. Інший спосіб — заволодіння номером телефону жертви та максимальному вилученні інформації під час телефонної розмови (починаючи від номера карти і закінчуючи добровільним назвою пін-коду, що приходить на телефон жертви). Потім отримується нова картка та передається шахраям, а номер телефону блокується.

Наявність відомостей про фінансову операцію, мобільний трафік, дає змогу правоохоронним органам встановити кінцевий пункт призначення вкрадених коштів. Окрім цього, можна встановити, де знаходився оператор, який дзвонив продавцеві, де був безпосередньо покупець під час дзвінка, можна встановити весь ланцюжок за допомогою простої аналітики разом із інформацією наданою оператором мобільного зв'язку і здійснення транзакцій коштів наданої банківською установою.

Отже, кібершахрайство є одним із поширених прикладів кіберзлочинів сьогодення. Практично усі види таких кримінальних правопорушень пов'язані з банківською системою, адже основна мета — незаконне збагачення за допомогою можливостей Інтернету. Серед причин, які сприяють поширенню цього виду кримінальних правопорушень, важливу роль відіграє ряд психологічних рис потенційної жертви кібершахрайства: віра у легку наживу, низький рівень критичного мислення та аналізу інформації (за допомогою якого потенційна жертва легко входить в довіру до шахрая), небажання звертатися до правоохоронних органів, ігнорування порад та застережень поліції та фахівців про запобіжні заходи тощо. Така поведінка громадян ще більше укорінює безкарність та поширення такого виду кримінальних правопорушень із все новітніми

способами різних афер із застосуванням засобів технічного прогресу.

Необхідно усвідомити нам усім, що розвиток сучасних технологій та вдосконалення методів заволодіння коштами шахрайським шляхом має тенденцію зростання, а тому, необхідно вдосконалювати профілактичні заходи для запобігання вчинення таких кримінальних правопорушень.

З приводу взаємодії приватних детективів і працівників поліції було б доцільним розробити відповідну інструкцію з метою відпрацювання алгоритму взаємодії і методики розслідування кримінальних правопорушень за участі приватних детективів, а саме: першочергові дії для перевірки наявної інформації про шахрайські схеми заволодіння коштами, подальшої її реєстрації і перевірки, а в разі її підтвердження - проведення ефективного розслідування із застосування класичних криміналістичних методів і новітніх технологій. Ці заходи дадуть змогу зменшити кількість ошуканих людей, підвищити якість розслідування кібершахрайств та їх профілактику.

1. Криминалистика: учебник / под ред. Е.П. Ищенко М.: Юристъ, 2000. 152 с. **2.** Єдиний звіт про кримінальні правопорушення по державі. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113281&libid=100820&c=edit&_c=fo#. **3.** Голіна В.В., Головкін Б.М. Кримінологія загальна та особлива частини: навч. посіб. Харків: Право, 2014. С. 332-347. **4.** Конвенція про кіберзлочинність. URL: http://zakon.rada.gov.ua/laws/show/994_575. **5.** Грібов М.Л. Розслідування шахрайства: питання законності проведення негласних слідчих (розшукових) дій. *Молодий вчений.* 2015. № 2 (17). С. 747-750. **6.** Офіційний сайт Департаменту кіберполіції Національної поліції Україниб URL: https://www.cyberpolice.gov.ua/. **7.** Детективные агентства & Частные детективы / Осторожно мошенники. URL: https://www.facebook.com/groups/detectivesworld/permalink/479788622214091/. **8.** Криміналістика: підручник / В.В. Пясковський, Ю.М. Чорноус, А.В. Іщенко, О.О. Алексеев та ін. Київ : Центр учбової літератури, 2015. 544 с. **9.** Основи кримінального аналізу: посібник з елементами тренінгу / О.Є. Користін, С.В. Албул, А.В. Холостенко, О.М. Заєць та ін. Одеса: ОДУВС, 2016. 112 с. **10.** Вікіпедія. URL: https://ru.wikipedia.org/wiki/%D0%9D%D0%B8%D0%B3%D0%B5%D1%80%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B5_%D0%BF%D0%B8%D1%81%D1%8C%D0%BC%D0%B0. **11.** Знакомства в Интернете: как не стать жертвой аферистов? 5 советов от экспертов «Касается каждого». URL: http://inter.ua/ru/news/2018/03/19/6522.

Kalinovsky Alexander, Bolgov Ruslan. **Application of classical criminalistic methods and modern technological opportunities in the private detective practice at investigation of kibershage**

The development of modern technology has given impetus to the emergence of crimes of a new generation — cybercrime. The most common types of cybercrime include, but are not limited to, various types of online fraud («Nigerian» letters, bank card fraud, fundraising for children with knowingly false photographs, etc.).

The purpose of this article is to highlight the peculiarities of the interaction of a private detective, journalists and Cyberpolice employees during the pre-trial investigation of several types of cyber-scam (using social networks, messengers, personal mail, mobile communication, advertisement sites and banking system) using classical methods of criminology and modern technologies.

The object of the study is: postings of knowingly false information (in social networks and messengers, SMS-messages), which were placed with the purpose of obtaining a monetary amount by abuse of trust, and «letters of happiness» or so-called «Nigerian letters» — the old way of fraud in the Internet system.

In the course of interaction of a private detective and representatives of the Cyberpolice of the National Police of Ukraine, the classical methods of criminology and modern technologies (generated links, photos from the ATM surveillance camera, etc.) gave an opportunity to detect cyber-shielding, identify suspects and initiate criminal proceedings. At present, further investigations and investigations are being conducted on these cases.

Cyber-fraud is one of the brightest examples of today's cybercrime. Virtually all kinds of such crimes circulate around the banking system, since the main goal is illegal enrichment through the use of the possibilities of the Internet. As long as people who sincerely believe in easy money, without checking the information received without listening to the advice of experts about the preventive measures - will thrive such fraudsters, to appear more and more ways of various scams, using the possibilities of technical progress.

Unfortunately, due to the lack of an institute of detectives in Ukraine, bureaucratic obstacles — the disclosure and prevention of such types of crime takes a lot of time, although technologies allow it to be done quickly. Currently, the capabilities of the private detective sector are significantly limited and, as a rule, are reduced to the timely detection and coverage of such fraudsters. For the prompt detection and illumination of this type of crime there is a constant interaction with representatives of banks and employees of the Cyberpolice, because timely intervention of Police officers in conjunction with the security service of the banking system helps to detect and prevent such a type of fraud.

Key words: *cybercrime, internet fraud, cybercrime, private detective, cyberpolice, pre-trial investigation.*