Додаток

КІБЕРЗЛОЧИННІСТЬ ТА ВІДМИВАННЯ КОШТІВ

ВСТУП

Сучасне суспільство - це суспільство інформаційних технологій, що базується на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без надійної роботи комп'ютерної техніки та засобів комунікацій. Інформаційні технології стали постійним супутником сучасної людини не лише на робочому місці, вони увійшли майже в усі сфери людського життя.

Розповсюдження нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та засобів комунікацій, оптимізації та автоматизації процесів в усіх без виключення сферах життєдіяльності, призвело разом з цим до нівелювання кордонів та переплетення національних економік та національних інфраструктур країн світу.

Більше того, вказані тенденції призвели до формування єдиного світового інформаційного простору, де кожен може отримати доступ до будь-якої інформації в будь-якій точці планети, здійснювати дистанційно управління власними активами та активами компанії, укладати господарські угоди з іноземними суб'єктами господарювання без необхідності особистого контакту тощо.

Разом з цим, інформаційний простір став місцем та в той же час й безпосередньо інструментом злочину. Відтепер злочин не потребує попередньої "обробки клієнта" та особистого контакту з потенційною жертвою. Головним інструментом злочинця стає лише комп'ютер та доступ до інформаційно-комунікаційних систем, де він за допомогою комп'ютерних вірусів та інших протизаконних технічних засобів одержує доступ до баз даних, банківських рахунків, автоматизованих систем управління.

Так, крадіжки даних платіжних карт (банківських рахунків) або даних доступу до системи інтернет-банкінгу з метою заволодіння коштами клієнтів банку, викрадення персональних даних та комерційної інформації з приватних комп'ютерів або серверів, умисне пошкодження роботи інформаційних систем або засобів комунікацій з метою створення збитків компаніям - це далеко не повний перелік подібних загроз, які несе з собою бурхливий розвиток сучасних інформаційних технологій, та відповідно виокремлюється в таке поняття як кіберзлочинність.

При цьому, кіберзлочинність набуває все більшого світового масштабу, новітні технології перетворюють реальних злочинців на анонімних, а легкість швидкого збагачення зваблює все більше людей долучитися до цієї злочинної діяльності.

Зокрема, за різними оцінками Інтернетом користується до 40 % населення планети (тобто близько 2,5 млрд. осіб) та при цьому кількість інтернет-користувачів як в усьому світі, так і в Україні, постійно зростає.

Популярність мережі Інтернет цілком закономірна, оскільки користувач має можливість: цілодобового доступу до значного обсягу інформації; швидкого обміну інформацією з іншими користувачами; проведення банківських, торгових, біржових операцій з будь-якого місця у зручний час та багато іншого.

Банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців.

Несанкціоноване списання коштів з банківських рахунків, шахрайство з платіжними картками, втручання в роботу інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS атаки на інтернет-ресурси, шахрайство в інформаційних мережах - це не вичерпний перелік кіберзлочинів, тобто злочинів у сфері інформаційних та комп'ютерних технологій. За оцінками експертів щорічні збитки від діяльності кіберзлочинців перевищують 100 млрд. дол. США.

Підготовка та скоєння кіберзлочину здійснюється практично не відходячи від "робочого місця", тобто такі злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна скоювати з будь-якої точки планети, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця.

Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу.

Вищевказані переваги даного виду злочину поряд з його значною прибутковістю стали безумовно суттєвими перевагами у порівнянні з іншими злочинами, скоєння яких в умовах удосконалення правоохоронних систем стає все важчим й вартісним.

Таким чином, проведення дослідження щодо основних схем та способів відмивання доходів, одержаних у сфері кіберзлочинності, на сьогодні є необхідним та актуальним. Основними питаннями, які будуть розглянуті в межах даного типологічного дослідження, є:

• визначення поняття кіберзлочинності та виявлення найбільш поширених способів вчинення кіберзлочинів;

• розгляд типових механізмів, методів та інструментів відмивання доходів, одержаних у сфері кіберзлочинності;

• систематизація критеріїв та ознак для своєчасного виявлення фінансових операцій, що можуть бути пов'язані з відмиванням доходів, одержаних у сфері кіберзлочинності;

• ознайомлення зі способами та методами протидії кіберзлочинам та відмиванню коштів, одержаних у сфері кіберзлочинності.

1. КІБЕРЗЛОЧИННІСТЬ: СУТЬ, ВИДИ, ЗАГРОЗИ ТА РИЗИКИ

1.1. Міжнародний та національний аспект боротьби з кіберзлочинністю

Питання пошуку шляхів упередження та протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги як державних органів, так й міжнародної спільноти.

Беручи до уваги, що розвиток технологій йде швидше ніж приймаються нормативно-

правові акти, якими вони регулюються, а об'єми незаконно одержаних коштів кіберзлочинцями зростають, необхідно на постійній основі знаходити шляхи вирішення нових задач, пов'язаних з такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних та обмін інформацією між державними та приватними структурами.

Міжнародна спільнота, враховуючи можливі негативні наслідки цього явища, знаходиться у постійному пошуку заходів, які дозволяють мінімізувати загрози впливу кіберзлочинності на суспільство. Останніми роками спостерігається значна активність в прийнятті міжнародних та регіональних документів, спрямованих на протидію кіберзлочинності, які включають як обов'язкові, так й необов'язкові до виконання вимоги.

Відповідно до дослідження, проведеного Управлінням Організації Об'єднаних Націй з наркотиків і злочинності на тему "Всебічне дослідження проблеми кіберзлочинності та відповідних заходів з боку країн-учасниць, міжнародної спільноти та приватного сектору", можливо виділити 5 груп документів, в які входять документи, розроблені в контексті або під егідою: I) Ради Європи чи Європейського Союзу; II) Співдружності незалежних держав або Шанхайської організації співробітництва; III) міжурядових африканських організацій; IV) Ліги арабських держав; V) Організації Об'єднаних Націй (далі - ООН). Всі ці документи в значній мірі доповнюють один одного, в тому числі в частині, що стосується концепцій та підходів, описаних в Конвенції Ради Європи про злочинність у кіберпросторі, прийнятій 23 листопада 2001 року в Будапешті, Угорщина (далі - Будапештська конвенція). На даний час Будапештська конвенція є фундаментом для розробки законодавства у боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства.

Будапештська Конвенція вимагає від держав:

- криміналізувати атаки на комп'ютерні дані і системи (тобто незаконний доступ, нелегальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями), а також правопорушення з використанням комп'ютерів (підробка і шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія) та правопорушення у сфері авторських і суміжних прав;

- вдосконалювати законодавство для того, щоб компетентні органи змогли проводити розслідування кіберзлочинів і зберігати електронні докази найефективніше, включаючи термінове збереження комп'ютерних даних, термінове збереження і часткове розкриття даних про рух інформації, обшук і арешт комп'ютерних даних, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації;

- розширювати міжнародне співробітництво з іншими країнами - учасницями Конвенції через загальні (екстрадиція, взаємна допомога, добровільне надання інформації тощо) і спеціальні заходи (термінове збереження та розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даних, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж тощо).

Комітет Конвенції проти кіберзлочинності (T-CY) був створений для того, щоб допомогти країнам-учасницям обмінюватися інформацією і розглядати необхідність внесення доповнень або протоколів до Конвенції.

Крім того, в 2006 році Рада Європи ініціювала Міжнародний проект по боротьбі з кіберзлочинністю, який направлений на те, щоб сприяти країнам в питаннях вдосконалення законодавства, навчання співробітників правоохоронних органів, органів прокуратури і

суддівського корпусу, зміцнення співпраці між державним і приватним сектором, вироблення заходів для захисту персональних даних, а також захисту дітей від сексуальної експлуатації та насильства.

Власну стратегію щодо вирішення проблем протидії кіберзлочинності розроблено також Європейським поліцейським відомством (Європол). На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів.

З січня 2013 року під егідою Європолу розпочав діяльність новий Європейський центр боротьби з кіберзлочинністю. Серед пріоритетів Центру - розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС.

Значну роль у подоланні проблем міжнародної співпраці у сфері боротьби з кіберзлочинністю відіграє ООН, яка приділяє достатню увагу питанням поширення злочинів, пов'язаних з використанням інформаційних та комп'ютерних систем, та боротьби з таким злочинами. ООН неодноразово наголошувала на транснаціональному характері кіберзлочинів та необхідності координації у світовому масштабі заходів щодо запобігання таким злочинам та їх розслідування.

У травні 2011 року Управлінням ООН з наркотиків і злочинності та Міжнародним союзом електрозв'язку було підписано угоду про боротьбу з кіберзлочинністю, спрямовану на розроблення правових рамок та юридичних механізмів протидії загрозам.

З метою обмеження загроз та незахищеності в інформаційному просторі Міжнародним союзом електрозв'язку, як спеціалізованою установою ООН, розроблено: Глобальну програму кібербезпеки; Вказівки для дітей щодо захисту в онлайновому середовищі; Вказівки для батьків, опікунів та вчителів щодо захисту дитини в онлайновому середовищі; Вказівки для галузі щодо захисту дитини в онлайновому середовищі; Вказівки для директивних органів щодо захисту дитини в онлайновому середовищі; Елементи для створення глобальної культури кібербезпеки.

Експертами Управлінням ООН з наркотиків і злочинності також зазначається, що форми міжнародного співробітництва включають видачу злочинців, надання взаємної правової допомоги, взаємне визнання іноземних судових рішень та неофіційне співробітництво між правоохоронними органами різних країн. Крім того, нестійкий характер електронних доказів в рамках міжнародного співробітництва в кримінальних питаннях у сфері кіберзлочинності вимагає своєчасного надання відповідей та наявності можливостей звертатися з проханням щодо проведення спеціалізованих слідчих дій, таких як збереження комп'ютерних даних.

На національному рівні попередження злочинності складається з стратегій і заходів, спрямованих на зниження ризику скоєння злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і суспільства. До числа оптимальних заходів в галузі попередження кіберзлочинності належать прийняття законів, стратегій протидії кіберзлочинності, ефективне керівництво, розвиток потенціалу органів кримінального правосуддя і правоохоронних органів, інформаційно-просвітницька діяльність, створення міцної бази знань і співробітництво між органами державного управління, громадами, приватним сектором і на міжнародному рівні.

На сьогодні в українському законодавстві відсутнє визначення поняття "кіберзлочин" або

"кіберзлочинність", є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку (розділ XVI Кримінального кодексу України (далі - КК України)), зокрема:

• несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України);

• створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361^1 КК України);

• несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361^2 КК України);

• 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 (стаття 362 КК України);

• 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 (стаття 363 КК України);

• перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363^1 КК України).

Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України - незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

1.2. Суть та види кіберзлочинів

Експертами Управлінням ООН з наркотиків і злочинності також зазначається, що визначення "кіберзлочинності" головним чином залежать від того, в яких цілях цей термін буде використовуватися. Основу кіберзлочинності становлять обмежене число діянь, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних даних або систем. Однак, якщо цим не обмежуватися, то щодо діянь, що передбачають використання комп'ютера в цілях отримання особистого або фінансового прибутку або заподіяння особистої або фінансової шкоди, включаючи форми злочинів, пов'язаних з використанням персональних даних, і діяння, пов'язані з інформацією, яка зберігається в комп'ютері (всі вони входять в більш широке поняття "кіберзлочинність"), досить проблематично знайти всеосяжне юридичне визначення.

У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов'язані з використанням інформації, яка міститься в комп'ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем.

Слід зазначити, що Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає умовну класифікацію кіберзлочинів, що поділяються на наступні категорії:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані "CIA-злочини"), зокрема:

• незаконний доступ, наприклад, шляхом злому, обману і іншими засобами;

• нелегальне перехоплення комп'ютерних даних;

• втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

• втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

• зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення "CIA-злочинів";

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

4) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад, незаконне відтворення і використання комп'ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і книг.

Згідно з класифікацією кримінальних злочинів, впроваджених КК України, поняття кіберзлочинності охоплює кримінальні правопорушення у сфері:

• використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем);

• обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

• господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж.

Водночас, з урахуванням мотивації злочинців, кіберзлочини вбачається за можливе умовно поділити на наступні категорії:

• кібершахрайство з метою заволодіння коштами;

• кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу);

• втручання в роботу інформаційних системи з метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам);

• інші злочини.

Перша категорія злочину - присвоєння коштів, при якому шахраї використовують різноманітні способи, іноді змушуючи користувачів самостійно розкривати конфіденційні дані.

За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів:

1) банкоматне шахрайство:

• скіминг - виготовлення, збут та встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї;

• використання "білого пластику" для "клонування" (підробки) платіжної картки та зняття готівки в банкоматах;

• Transaction Reversal Fraud - втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником;

• Cash Trapping - заклеювання диспенсеру для привласнення зловмисником готівки, яка була списана з карткового рахунку законного держателя картки;

2) шахрайство в торгівельно-сервісних мережах:

• укладання фіктивних угод торговельного еквайрінгу для обслуговування підроблених платіжних карток;

• викрадення реквізитів платіжних карток, у тому числі із застосуванням технічних засобів їх "клонування";

• операції на суму нижче встановленого ліміту без проведення авторизації;

• використання втрачених/викрадених/підроблених платіжних карток;

3) шахрайство в мережі Інтернет:

• викрадення реквізитів платіжних карток;

• проведення операцій із використанням викрадених реквізитів платіжних карток;

• діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток (створення фіктивних WEB-сайтів, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).

4) шахрайство в системах дистанційного банківського обслуговування (далі - ДБО):

• створення комп'ютерних вірусів та троянських програм для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням ДБО;

• відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті несанкціонованих операцій у системах ДБО;

• отримання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання у роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.

Найпоширеніші злочини, які відносяться до другої та третьої категорії - це злом баз даних та виведення з ладу комп'ютерних систем компаній і урядових організацій.

Також широко розповсюдженими є крадіжки інновацій або технологій і, звичайно, банальна крадіжка грошей. Одна із найбільш поширених схем, коли шахраї крадуть дані зарплатних рахунків співробітників компаній, які в подальшому продають їх на чорному ринку. Розцінки на таку специфічну інформацію починаються від кількох доларів США за рахунок. Є й інший варіант - залишити ці дані собі й просто перевести гроші з сотень і тисяч банківських карт на свій рахунок.

У межах даного дослідження найбільш детально розглянуто кіберзлочини, що здійснюються з метою або внаслідок яких виникає фінансова або інша матеріальна вигода у вигляді незаконно одержаних доходів. В першу чергу, мова йде про використання інформаційно-комунікаційних систем та комп'ютерних технологій для доступу до приватної власності юридичних та фізичних осіб та подальших дій щодо управління чи розпорядження цією власністю. Зокрема, найбільшого розповсюдження на сьогодні серед кіберзлочинів набрало одержання доступу до коштів клієнтів банківських установ.

Слід зазначити, що стрімкий розвиток сфери інформаційних технологій постійно генерує нові види послуг, в тому числі у фінансовій сфері. Це, в свою чергу, змушує злочинців вдосконалювати свої здібності та вигадувати нові способи незаконного заробітку в кіберсередовищі.

1.3. Загрози та ризики, пов'язані із кіберзлочинами

У типологічному дослідженні MONEYVAL "Кримінальні грошові потоки в мережі Інтернет: методи, тенденції та взаємодія між всіма основними учасниками" розглянуто наступні ризики кіберзлочинності і відмивання злочинних доходів:

• технічні ризики;

• операційні ризики;

• юридичні ризики;

• географічні або юрисдикційні ризики.

Водночас, така класифікація є дещо узагальненою та потребує більш детального розгляду з урахуванням суті загроз та вразливостей суспільству і державі від кіберзлочинності, наслідків їх реалізації та можливостей їм протистояти чи зменшувати їх вплив.

Виходячи із суті та класифікації кіберзлочинів, можливо виділити наступні загрози суспільству та державі:

- відкритість суспільства та держави.

Створена на основі комп'ютерних мереж та інформаційних технологій зручна інфраструктура для міжнародних постачань товарів, надання послуг, переказу коштів між фізичними і юридичними особами, зберігання інформації у мережі Інтернет та під'єднання до неї кожного комп'ютера надає одночасно широкі можливості як власне кіберзлочинів, так і відмивання грошей від цих або інших злочинів за допомогою комп'ютерних технологій;

- швидкість та невисока вартість злочину.

Вищевказана інфраструктура також надає можливість злочинцям швидкого доступу до

будь-якої інформації, документів та насамкінець приватної власності, і водночас дешевих, оперативних і практично анонімних платіжних систем, що дозволяє швидко, без додаткових витрат та ефективно приховати сліди злочину та подальшого руху незаконно одержаних доходів;

- висока технологічність.

Надзвичайно швидкий розвиток інформаційних технологій та складність цієї сфери поряд з відносно тривалим та бюрократичним підходом до розвитку нормативно-правових баз призводить до значного відставання заходів щодо упередження та боротьби з кіберзлочинністю;

- складний характер злочину.

Окрім того, що кіберзлочинці одержують фінансові або інші матеріальні вигоди від здійснення злочину, вони використовують комп'ютерні технології, інформаційно-комунікаційні мережі з соціально-психологічних міркувань, зокрема, дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, псування і руйнування ключових систем шляхом внесення до них фальсифікованих даних або постійного виведення цих систем з робочого стану (що є свого роду доповненням до традиційного виду тероризму);

- анонімність злочину.

Злочинців приваблює відсутність фізичного контакту з жертвою, відносна м'якість покарання в деяких країнах та, безперечно, складність виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі;

- транснаціональний та популярний характер злочину.

Особливістю даного виду злочинності є те, що підготовка та скоєння злочину, за наявності доступу до мережі Інтернет, може здійснюватись практично з будь-якого місця. А враховуючи, що комп'ютерна техніка та Інтернет-послуги стають доступнішими для все ширшого кола осіб, кіберзлочинність стає все більш популярною.

Транснаціональне функціонування надає злочинцям дуже привабливі можливості, тобто вони можуть здійснювати свою діяльність з територій тих юрисдикцій, в яких недостатньо розвинений режим протидії кіберзлочинам, а також відмиванню доходів та фінансуванню тероризму і відповідний нагляд, а також, де вони не стануть суб'єктами розслідування, що проводиться іноземними правоохоронними органами.

Деякі країни використовуються як транзитні вузли, тобто грошові потоки йдуть в ці країни, але в той же час грошові потоки з цих країн розтікаються по інших напрямах, деякі з них нехарактерні для кібератак;

- організований характер та змішаний склад учасників злочину.

У сучасних умовах масштабні успішні кіберзлочини можливо скоювати лише за умов відповідної організації та підготовки, яка носить фактично організований злочинний характер. Дії кіберзлочинців націлені головним чином на отримання надприбутків, що відповідно призводить до збільшення кількості комп'ютерних злочинів саме у фінансовій сфері, що потребує розуміння сфери фінансових відносин та банківської діяльності. При цьому кіберзлочинці активно співпрацюють з представниками традиційної злочинності, які допомагають першим трансформувати викрадені кошти у готівку.

Всі вищевказані загрози призводять до появи та розвитку вразливостей системи протидії

кіберзлочинам, що в першу чергу пов'язані з:

- вчасністю виявлення кіберзлочинів;

- тривалістю та складністю розслідування і використання доказів (зокрема в електронній формі) в судовому провадженні.

Певні характеристики електронних платіжних систем можуть бути факторами ризику відмивання злочинних доходів. Відносна легкість створення електронних платіжних систем поряд з низькими витратами на розвиток такої діяльності породжує сумніви щодо власника. Швидкість, з якою проводяться операції, включаючи транскордонні перекази, лише сприяють реалізації схем відмивання злочинних доходів. Низька вартість таких операцій означає і низьку вартість послуг з відмивання і стимулює злочинців на пошук незаконних джерел отримання прибутку. Легка конвертація в реальні гроші та готівку може представляти можливість для відмивання грошей у багатьох юрисдикціях.

Наслідком значної кількості кіберзлочинів у вказаній сфері є зниження довіри громадян в цілому до надійності фінансової системи, інституту банківської таємниці, надійності захисту персональних даних, а також до фінансових операцій, що проводяться з використанням новітніх технологій. При цьому недовіра населення до ринків фінансових послуг не дає можливості активно використовувати вільні кошти громадян як інвестиційні ресурси, що спрямовуються на розвиток економіки.

В цілому такі наслідки можливо розділити на наступні групи:

• фінансові - втрата коштів банківськими установами та їх клієнтами (юридичним та фізичними особами);

• іміджеві (репутаційні) - розкриття конфіденційної інформації, у тому числі банківської таємниці та персональних даних; недовіра клієнтів до банківської системи в цілому, та систем ДБО зокрема, що тягне за собою зменшення обсягу безготівкових операцій;

• юридичні - позови клієнтів;

• технологічні - з метою забезпечення надійної роботи інформаційних, комп'ютерних та телекомунікаційних систем банківські установи, підприємства та організації змушені створювати (або придбавати) складніші, дорожчі та менш зручні у використанні засоби захисту.

2. КРИМІНАЛЬНІ ДОХОДИ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

2.1. Шахрайство в системах дистанційного банківського обслуговування

В сучасних умовах системи ДБО (Клієнт-Банк, Інтернет-Клієнт-Банк, Інтернет-банкінг тощо) стали невід'ємною частиною фінансової системи як в Україні, так і у всьому світі.

Дистанційне банківське обслуговування (ДБО) - загальний термін для технологій надання банківських послуг на підставі розпоряджень, переданих клієнтом віддалено (без візиту до банку).

Система ДБО - це багатофункціональний програмно-технічний комплекс, що дозволяє клієнтам банку готувати і направляти в банк на виконання платіжні та інші документи, контролювати стан своїх рахунків, а також отримувати широкий спектр актуальної фінансової інформації без безпосереднього звернення до банку.

Використання системи ДБО безперечно має свої переваги. Насамперед, слід виділити наступні:

• оперативність та економічність. Використання системи ДБО дозволяє з офісу здійснювати управління фінансовими потоками підприємства й істотно скорочує витрати робочого часу персоналу, пов'язані з відвідуванням банку;

• простота і зручність. Автоматизація процесу підготовки платіжних та інших документів, а також наявність програмного контролю щодо заповнення обов'язкових реквізитів у документах значно спрощує користування підсистемами і дозволяє мінімізувати операційні помилки;

• безпека та ефективність. Система 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.

В той же час, системи ДБО, як інструмент доступу до грошових переказів, сьогодні все частіше стають мішенню для кіберзлочинців.

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.

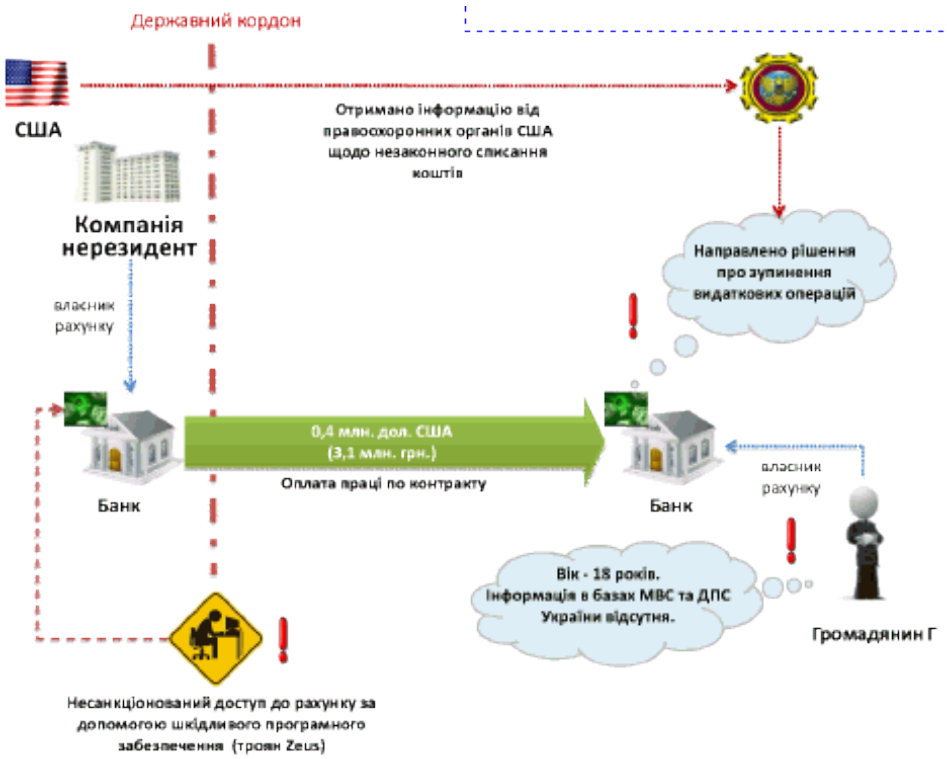
Завантаження вірусу на комп'ютер жертви відбувається практично непомітно. Основне завдання вірусу на початковому етапі - це спостереження, збір інформації і передача його на комп'ютер шахраїв. Вірус може викрадати паролі доступу до систем ДБО, ключі електронного цифрового підпису, зчитувати реквізити 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.

Приклад

На рахунок громадянина України Г від імені компанії-нерезидента, зареєстрованої на території США, зараховано грошові кошти в сумі 0,4 млн. дол. США (3,1 млн. грн.) як оплата праці по контракту.

Водночас, отримувач коштів - громадянин Г - є особою молодого віку (18 років), місця одержання доходу не має, господарською діяльністю не займається.



За інформацією правоохоронних органів США кошти було перераховано в результаті втручання невідомої особи в комп'ютерну мережу компанії-нерезидента з використанням шкідливого програмного забезпечення - трояна Zeus.

З урахуванням інформації правоохоронних органів США Держфінмоніторингом України прийнято рішення щодо зупинення фінансових операцій по рахунку громадянина України.

Кримінальне провадження відкрито за ч. 1 ст. 190 "Шахрайство" КК України. Слідство триває.

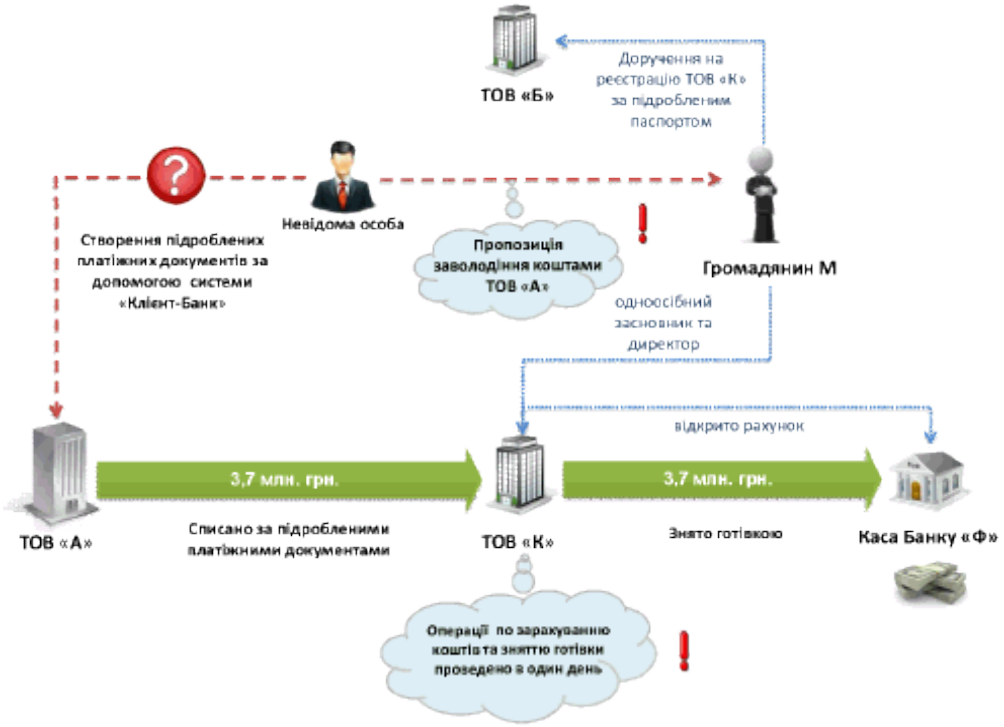
Приклад

Громадянин М познайомився з невстановленою слідством особою, яка запропонувала йому взяти участь у заволодінні коштами ТОВ "А" шляхом обману, на що він погодився.

У подальшому громадянин М з метою виконання свого злочинного наміру, використовуючи завідомо підроблений паспорт, виданий іншій особі, звернувся до офісу ТОВ "Б" з метою реєстрації ТОВ "К" як директор та єдиний засновник.

Для здійснення незаконної діяльності, пов'язаної із заволодінням коштами ТОВ "А", уповноважив працівників ТОВ "Б" бути його представниками в усіх установах та організаціях незалежно від форм власності з питань проведення державної реєстрації.

У подальшому зареєстровано ТОВ "К" та відкрито поточний рахунок у банку "Ф".



Невстановлена слідством особа за допомогою системи "Клієнт-Банк" створила підроблені платіжні документи на переказ коштів в сумі 3,7 млн. грн. з рахунку ТОВ "А" на рахунок ТОВ "К".

У цей же день громадянин М, як директор ТОВ "К", звернувся до банку "Ф" та за підробленими грошовими чеками отримав в касі вказаного банку кошти у сумі 3,7 млн. грн.

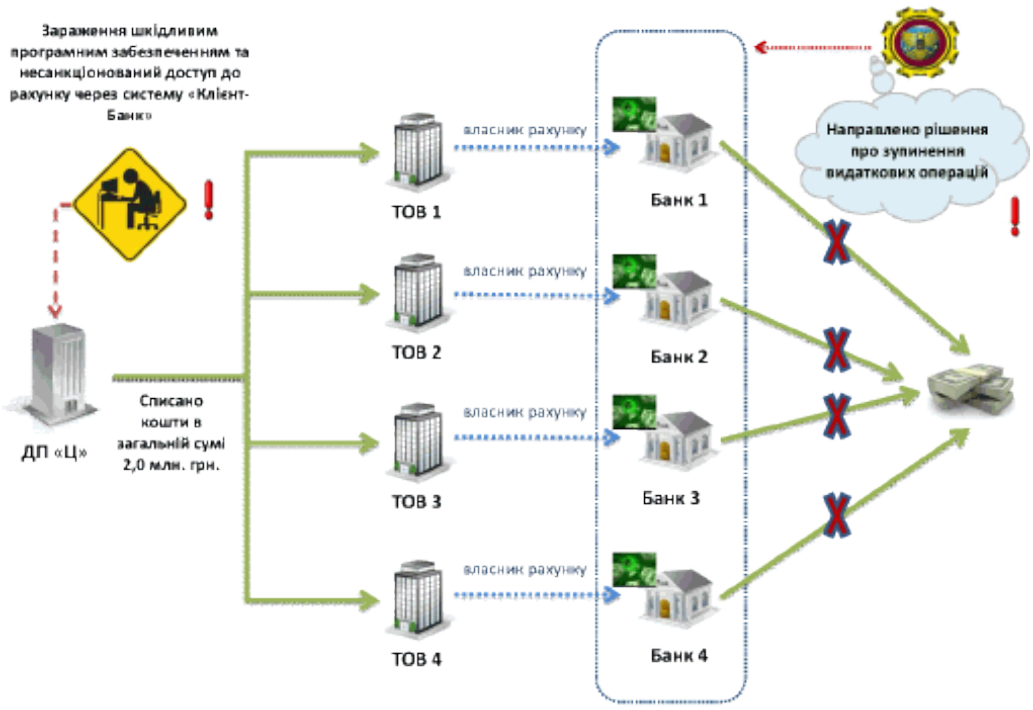
Вироком суду громадянина М визнано винним у вчиненні злочинів, передбачених ч. 4 ст. 190 "Шахрайство", ч. 2 ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення", ч. 1 ст. 205 "Фіктивне підприємництво" КК України та призначено покарання у вигляді 8 років позбавлення волі з конфіскацією всього майна.

У подальшому ухвалою апеляційного суду призначене покарання громадянину М за ч. 4 ст. 190 "Шахрайство" КК України до 6 років позбавлення волі з конфіскацією всього майна.

Приклад

Правоохоронним органом виявлено факт несанкціонованого втручання в систему "Клієнт-Банк" ДП "Ц" та незаконного перерахування з розрахункового рахунку вказаного підприємства коштів в сумі 2,0 млн. грн. на рахунки чотирьох підприємств, відкритих в різних банках.

За даним фактом розпочато кримінальне провадження за ознаками злочину, передбаченого ч. 2 ст. 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку" КК України.



В ході досудового слідства встановлено, що комп'ютер ДП "Ц", на якому встановлено систему "Клієнт-Банк", був уражений шкідливим програмним забезпеченням, і через видалений доступ зловмисники, використовуючи електронні ключі з цифровими підписами посадових осіб сформували та відправили відповідні платіжні доручення від імені цього підприємства. Комп'ютер вилучено та направлено на дослідження.

Працівниками правоохоронного органу терміново надано інформацію до Державної служби фінансового моніторингу України, якою зупинено видаткові операції по рахунках вказаних суб'єктів підприємницької діяльності.

Слідство триває.

2.2. Підробка платіжних карток та банкоматне шахрайство

Платіжні картки в сучасних умовах є не лише засобом для отримання заробітної плати, пенсії або інших зарахувань, але й ефективним та зручним інструментом для повноцінного банківського обслуговування.

Використання платіжних карток дає змогу:

• зменшити обсяги використання готівки;

• додатково захистити грошові кошти (при втраті картки грошові кошти блокуються та залишаються на рахунку держателя картки);

• проводити операції не тільки в національній, але в іноземній валюті (мультивалютні картки);

• проводити розрахунки цілодобово та в різних країнах світу.

Ринок платіжних карток зростає в Україні досить швидкими темпами (понад 20 % на рік). Так, за інформацією Національного банку України станом на 1 жовтня 2013 року в Україні перебуває в обігу 68,1 млн. платіжних карток, з яких 33,9 млн. карток є активними.

При цьому сума операцій, проведених з використанням платіжних карток, за 9 місяців 2013 року становить близько 650,0 млрд. грн.

Значні обсяги фінансових операцій з використанням платіжних карток є основним чинником, який привертає до цієї сфери особливу увагу злочинців. З метою заволодіння коштами держателів платіжних карток злочинці вигадують найрізноманітніші способи. Це, зокрема, можуть бути:

• технічні пристрої, які встановлюються на банкомат з метою заволодіння платіжною карткою або грошима;

• електронні пристрої, які дозволяють зчитувати необхідну інформацію з платіжної картки або з клавіатури банкомата;

• зараження комп'ютерів спеціалізованими вірусами з метою отримання інформації щодо платіжних карток (шляхом підробки або злому сайтів, використання бот-мереж та розсилки шкідливого спаму);

• підробка платіжних карток з використання викраденої інформації;

• телефонне шахрайство (коли злочинці видають себе за співробітників банку та намагаються отримати необхідну інформацію).

Існує безліч видів шахрайства з платіжними картками та банкоматами (фішинг, фармінг, трешинг, скіминг, траппінг, фантом, шаттер, шиммінг тощо), але всі вони направлені на викрадення безпосередньо грошових коштів, платіжної картки або її реквізитів, таких як:

• номер картки;

• дата випуску / завершення дії картки;

• код CVV2 (тризначне число на звороті платіжної картки служить кодом підтвердження операцій, що здійснюються в мережі Інтернет або за допомогою телефону);

• написання прізвища та імені клієнта латиною;

• ПІН-код.

При цьому, викрадена інформація може бути використана злочинцями не тільки для підробки платіжної картки або списання коштів, але й виставлена на продаж на спеціалізованих сайтах або форумах.

Приклад

Громадянин М з метою заволодіння чужим майном шляхом обману, використовуючи електронно-обчислювальну техніку через мережу Інтернет замовив на ім'я громадянина Б телевізор марки "Самсунг", за який здійснив перерахування коштів на рахунок ФОП "К" із використанням реквізитів банківської картки, яка належить невстановленій слідством особі і, відповідно, яка не належала громадянину М.

У цей же день телевізор марки "Самсунг" вартістю 16,6 тис. грн. отримав громадянин Б, який сплатив громадянину М кошти в сумі 7,0 тис. грн., оскільки останній повідомив громадянину Б неправдиву інформацію про те, що він домовився з продавцем щодо продажу товару за заниженою ціною. Таким чином, громадянин М розпорядився даним майном на власний розсуд.

Крім того, громадянин М з метою заволодіння чужим майном шляхом обману, використовуючи електронно-обчислювальну техніку через мережу Інтернет, повторно замовив телевізор марки "Самсунг" та ноутбук, за який здійснив перерахування коштів на рахунок ФОП "К" із використанням реквізитів банківської картки, яка належить невстановленій слідством особі і, відповідно, яка не належала громадянину М.

В цей же день за місцем мешкання громадянина М було доставлено замовлену продукцію на суму 14,4 тис. грн., якою громадянин М розпорядився на власний розсуд.

У подальшому банківською установою, через яку проходили несанкціоновані операції, підтверджено незаконність перерахування коштів, в результаті чого ФОП "К" завдано майнової шкоди на вищевказані суми.

Вироком суду громадянина М визнано винним у вчинені злочину, передбаченого ч. 3 ст. 190 "Шахрайство" КК України, та призначено йому покарання у вигляді 4 років позбавлення волі, але в силу ст. 75 "Звільнення від відбування покарання з випробуванням" КК України звільнено від відбування покарання з випробуванням, встановивши іспитовий строк 3 роки.

Приклад

До правоохоронних органів звернувся директор банківської установи щодо несанкціонованого встановлення зчитувальних пристроїв на банкомати зазначеного банку та подальшого зняття грошових коштів з карткових рахунків клієнтів.

В результаті оперативних заходів був затриманий на місці злочину громадянин Республіки Болгарія, який з метою викрадення грошей з банківських рахунків шляхом використання підроблених платіжних карток встановлював саморобні пристрої для зчитування інформації з банкоматів вказаної банківської установи.

В ході проведення досудового слідства встановлено, що зловмисник входив до злочинної групи в кількості 5 громадян Болгарії, які скоювали аналогічні злочини на території України та держав СНД.

Також було викрито та затримано на місці скоєння злочину іншого члена вказаної злочинної групи - громадянина Республіки Болгарія, який з метою незаконного зняття

грошових коштів з банківських рахунків шляхом використанням підроблених платіжних карток несанкціоновано встановив саморобні пристрої для зчитування інформації з банкоматів іншої банківської установи.

За місцем його тимчасового мешкання у номері готелю були вилучені саморобні пристрої для зчитування інформації з платіжних карт.

Кримінальні провадження відкрито за скоєння злочинів, передбачених ч. 3 ст. 190 "Шахрайство" та ч. 1 ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення" КК України.

Приклад

Правоохоронним органом в ході досудового слідства встановлено, що групою громадян Румунії на вхідних дверях банківської установи встановлено скімінговий пристрій, призначений для зчитування магнітної полоси банківської платіжної картки, та відеокамеру для зняття інформації про пін-коди карток. В подальшому зазначені громадяни виготовили дублікати банківських платіжних карток, емітованих українськими банками та зняли в банкоматах з рахунків клієнтів банківської установи грошові кошти в сумі 14,7 тис. грн.

Під час спроби зняття встановленого скімінгового пристрою двох громадян Румунії було затримано.

Вироком суду вищезазначених громадян засуджено за ч. 2 ст. 185 "Крадіжка", ч. 3 ст. 190 "Шахрайство", ч. 2 ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення", ст. 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю" та винесено вирок у вигляді 3 років позбавлення волі та штрафу у розмірі 85,0 тис. грн. кожному.

Приклад

Громадянка Бразилії С та громадянин Бразилії Д встановили скімінговий пристрій, призначений для зчитування магнітної полоси банківської платіжної картки на одному з банкоматів, що розташовані на території міста Києва.

В подальшому, використовуючи отриману при вказаних обставинах інформацію про банківські платіжні картки, зазначені громадяни виготовили дублікати банківських платіжних карток, емітованих українськими банками, і у подальшому здійснили 170 операцій, використавши при цьому 25 різних підроблених банківських платіжних карток.

Крім того, при черговій спробі здійснення незаконної фінансової операції, а саме зняття грошових коштів у сумі 62,2 тис. грн. за допомогою дубліката (підробленої) банківської платіжної картки з банкомата банку "К", було затримано громадян Бразилії С та Д, у яких було вилучено 25 підроблених банківських платіжних карток, скімінговий пристрій та 1,0 тис. грн.

Судом визнано винним громадянина Бразилії Д у скоєнні злочину, передбаченого ч. 1 ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення" КК України, та призначено покарання у вигляді штрафу у розмірі 51,0 тис. грн.

2.3. Шахрайство з використанням комп'ютерних технологій та інформаційно-комунікаційних систем

В межах даного дослідження, під кібершахрайством розуміється шахрайство, здійснене з використанням комп'ютерів, комп'ютерних мереж, в тому числі з використанням мережі Інтернет.

Слід зазначити, що в сучасних умовах значна частина традиційного бізнесу переходить у віртуальне середовище, що пояснюється стрімким розвитком мережі Інтернет. Це насамперед стосується розміщення в мережі Інтернет реклами товарів і послуг та Інтернет-торгівлі, яка є достатньо розповсюдженою в Україні та, у певних сферах, складає значну конкуренцію традиційній торгівлі.

Шахраї так само використовують сучасні можливості мережі Інтернет для своїх оборудок. Досить розповсюдженими є:

• шахрайство при продажу товарів через Інтернет або на Інтернет-аукціонах (створення сайтів - двійників відомих інтернет-магазинів, продаж неіснуючих або підроблених товарів та послуг тощо);

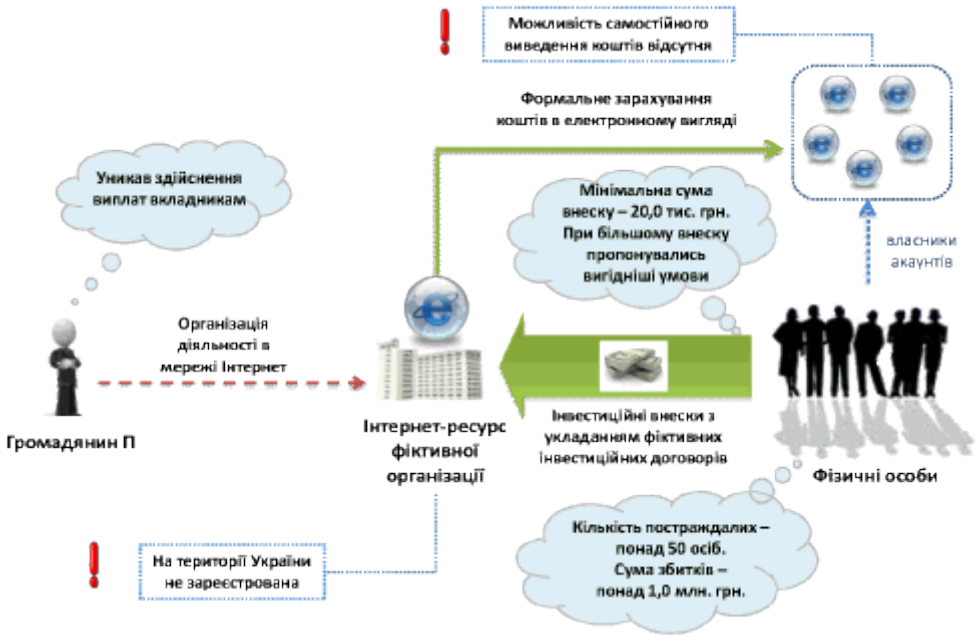
• створення "фінансових пірамід" в мережі Інтернет;

• розміщення шахрайських оголошень щодо збору коштів (благодійні пожертви) та ін.

Приклад

Громадянин П з 2009 року під виглядом здійснення законної діяльності філії Інвестиційної фондової біржі "К" залучав осіб для внесення грошових коштів з метою проведення ринкової трейдерської діяльності на веб-сайті мережі загального доступу Інтернет.

Особам, що вступили до Інвестиційної фондової біржі "К", пропонувалось отримання можливості одержати фінансову вигоду не тільки від особистого вкладу, але й за рахунок залучення до фінансової піраміди грошових коштів інших осіб.



Для вступу до біржі у якості ринкового трейдера учасникам необхідно було здійснити внесок у розмірі 20,0 тис. грн. При внеску, більшому за вказану суму, трейдерам пропонувались більш вигідні умови при здійсненні діяльності.

Після укладання фіктивного інвестиційного договору з учасниками, останнім на власні акаунти зараховувались кошти в електронному вигляді, однак вони мали лише формальний характер. Самостійно перевести зароблені грошові кошти у готівку вкладники не мали змоги. При зверненні трейдерів до громадянина П з вимогою виплати зароблених коштів або повернення вкладених грошових коштів, останній уникав здійснення виплат.

Інвестиційна фондова біржа "К" та її філії на території України не зареєстровані.

Більше 50 потерпілим особам від незаконної діяльності спричинено збитків на суму понад 1,0 млн. грн.

Приклад

Правоохоронним органом виявлено групу шахраїв, які заволодівали коштами громадян під виглядом реалізації товарів на інтернет-аукціонах.

При проходженні реєстрації у якості продавця товару на Інтернет-сайті зловмисники зазначали дані (П. І. Б., ідентифікаційні коди, місця проживання, номери банківських карток, інше) сторонніх осіб.

Зазначені дані вони заздалегідь отримували з місць позбавлення волі Вінницької області.

Окрім того, для реєстрації кожного нового акаунту винаймали у різних містах України квартири з обов'язковою наявністю в них підключення до мережі Інтернет.

Також, для приховування своєї особистості, під час оренди кожної наступної квартири надавали власникам помешкання підроблені документи, що посвідчують особу, а при кожній реєстрації в Інтернет-аукціоні використовували нову комп'ютерну техніку та користувались послугами понад 10 Інтернет-провайдерів різних регіонів України.

Встановлена кількість потерпілих з усіх регіонів України складає 140 осіб.

Приклад

В результаті моніторингу мережі Інтернет правоохоронним органом було отримано інформацію про злочинну діяльність ряду осіб, пов'язану з шахрайським залученням грошових коштів громадян.

Група осіб в мережі Інтернет розробила, організувала та адмініструвала On-line ресурс "А", в якому під виглядом агентства із залученням інвестицій організовано діяльність "фінансової піраміди".

Схема вказаної злочинної діяльності передбачала залучення грошей громадян під виглядом фінансових інвестицій з можливістю отримання прибутків у вигляді дивідендів та подарунків, а саме квартир, автомобілів і різних побутових товарів. У міру збільшення кількості інвесторів при наявності достатнього обсягу інвестицій здійснено одиничні виплати "дивідендів" окремим учасникам. При досягненні моменту, коли кількість необхідних виплат перевищувала кількість залучених коштів, діяльність фінансової піраміди припинена.

150 потерпілих жителів СНД прийняли участь в інвестиційному проекті "А" та вклали кошти в сумі понад 0,5 млн. грн.

В результаті проведених в офісі та за місцем проживання організаторів піраміди обшуків було вилучено комп'ютерну техніку, на якій розміщена база учасників піраміди (загальна чисельність перевищує 8 тис. осіб), а також документація про фінансову діяльність інвестиційного проекту.

За фактом шахрайських дій було зареєстровано кримінальне провадження, за ознаками злочину, передбаченого ч. 3 ст. 190 "Шахрайство" КК України.

Приклад

Громадянин А у соціальній мережі "Вконтакте" розмістив оголошення про виготовлення та монтаж пластикових вікон.

Не маючи наміру виконувати зобов'язання, громадянином А отримано від замовників передоплати в сумі близько 25 тис. грн.

Розслідування триває.

Приклад

Група осіб під приводом перерахування значних грошових коштів на лікування онкохворих дітей дізнавалась у батьків дані банківських карток.

Зазначені особи телефонували автору оголошення, яке знаходили в Інтернеті, і говорили, що готові допомогти, але їм необхідно надати реквізити платіжної картки.

Громадяни довірливо ставились до такої пропозиції, повідомляли шахраям інформацію про термін дії картки, коди підтвердження тощо.

Зловмисники через електронну платіжну систему заповнювали реквізити, які вони отримали у потенційного потерпілого, спеціально помилково вводили один з кодів, який є паролем.

Система надсилала інформацію про введення неправильного коду повідомлення господарю картки на його мобільний телефон.

Після цього злочинці замовляли через програму, щоб їм надіслали, пароль ще раз, бо вони нібито його забули.

Банківська система налаштована так, що з метою підтвердження реального платника, припускаючи, що мобільний телефон знаходиться у справжнього власника картки, надає команду на зміну пароля, код доступу для зміни пароля приходить на телефон господаря картки.

Після цього злочинці телефонували йому і просили повідомити СМС-повідомлення, яке прийшло - тобто, підтвердження на зміну пароля. Мотивували тим, що їм це необхідно для завершення операції та миттєвого перерахування грошей на рахунок.

В подальшому шляхом технічних маніпуляцій від імені потерпілих злочинці перераховували кошти на картки учасників злочинної групи та знімали готівкою з банкоматів.

В ході досудового слідства встановлені організатор та двоє співучасників злочинної групи. Їм повідомлено про підозру в скоєнні кримінальних правопорушень за ознаками злочину, передбаченого ч. 3 ст. 190 "Шахрайство" КК України по 32 епізодам.

Також встановлені ще двоє організаторів злочинної групи, які відбували покарання в місцях позбавлення волі, звідки й здійснювали злочинні дії. Їм також повідомлено про підозру в скоєнні злочину, передбаченого ч. 3 ст. 190 "Шахрайство" КК України по 31 епізоду.

Загальна сума збитків, нанесених діяльністю злочинної групи постраждалим, складає близько 500 тис. грн.

Приклад

Громадяни України, Кіпру, Італії, Ізраїлю та невстановлені особи, які розподілили між собою ролі, організували у всесвітній мережі Інтернет казино, на якому в режимі онлайн у реальному часі ведеться гра у такі азартні ігри як покер, блекджек, рулетка.

Так громадянин Італії та інші невстановлені особи здійснювали фінансування даного проекту, громадянин Ізраїлю забезпечував роботу програмних комплексів, громадянин Кіпру контролював роботу ігрової зали, а громадянин України утримував та організовував роботу зали, а також здійснював набір дівчат для роботи круп'є.

Під час гри використовувалися програмні комплекси, які автоматично зчитують гральні карти та місце знаходження шарику на рулеточному столі. Ставки приймались від громадян усього світу, включаючи Україну. Програмне забезпечення автоматично визначало виграш або програш ставок, а круп'є перед веб-камерами здійснювали роздачу гральних карт та керували рулеткою.

Встановлено, що головний сервер, який розташований у Великобританії, являється базовою платформою для ресурсів, які надають послуги власникам гральних Інтернет-ресурсів або залів, як у місті Києві, так і за кордоном.

Відносно осіб, що входили в організовану групу, порушено кримінальну справу за ознаками складу злочину, передбаченого ст. 203^{2} "Зайняття гральним бізнесом" КК України.

В ході проведення обшуку в приміщенні ігрової зали під час проведення гри затримано на гарячому громадянина Кіпру.

Разом з ним затримано 24 круп'є та 3 системні адміністратори, які здійснювали забезпечення роботи комп'ютерів. Вилучено 19 гральних столів, обладнаних сканерами штрих-кодів, відеокамерами, направлених на круп'є, та монітори, де видно ніки гравців та ставки, 22 персональні комп'ютери, серверне обладнання та документи, які підтверджують причетність вказаних осіб до вчинення даного злочину.

2.4. Кіберзлочинність нефінансового характеру

В межах даного дослідження до кіберзлочинів нефінансового характеру віднесено злочини у кіберпросторі, що безпосередньо не стосуються сфери фінансових послуг та переказу коштів. Однак, отримання незаконних доходів є основною метою скоєння і цих злочинів.

До таких злочинів слід віднести:

• виведення з ладу комп'ютерів та комп'ютерних мереж (DDoS-атаки на сайти, блокування роботи конкурентів тощо);

• викрадення ділової або особистої інформації;

• кіберздирництво, залякування, наклеп та поширення неправдивої інформації в мережі

Інтернет;

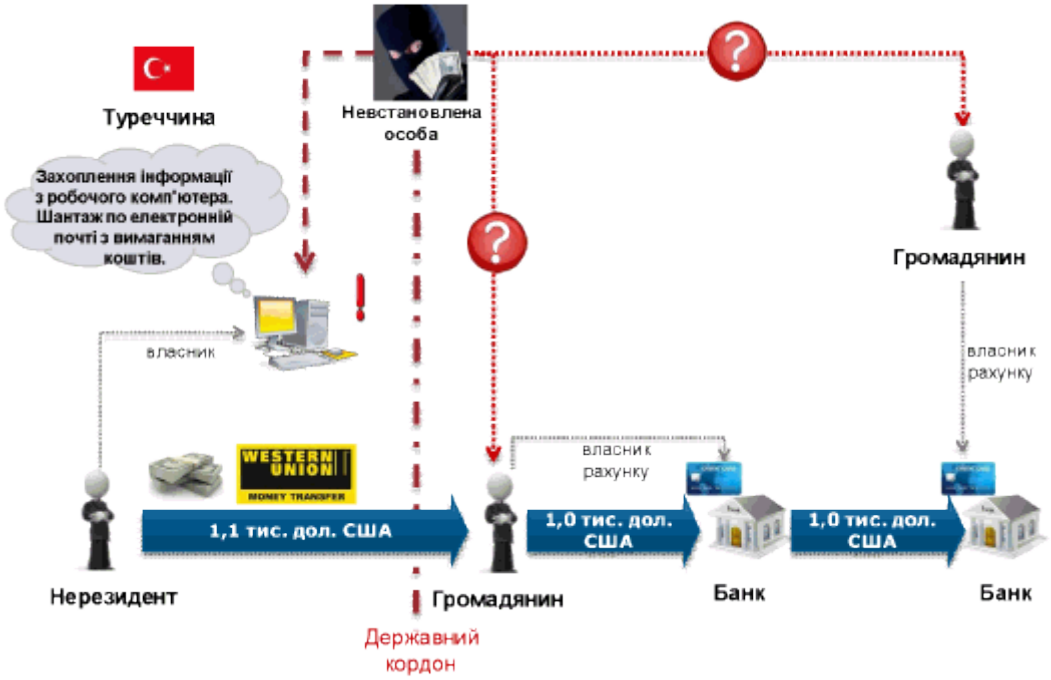
• проведення заборонених азартних ігор он-лайн;

• порушення авторських та суміжних прав шляхом незаконного відтворення і використання комп'ютерних програм, розміщення в мережі Інтернет аудіо/відео та інших видів цифрової продукції;

• злочини, пов'язані з вмістом даних, зокрема дитяча порнографія, дитяча експлуатація і сексуальне насильство, расизм, ксенофобія.

Приклад

Групою осіб організовано комп'ютерні атаки та викрадено бізнес-інформацію з робочих комп'ютерів громадян Туреччини, США та Німеччини.



В подальшому, за повернення викраденої інформації вимагалися грошові кошти, які були надіслані в Україну через Western Union на користь організатора схеми та зняті готівкою з карткового рахунку довіреною особою.

Загальна сума отриманих фізичними особами коштів становить 20,0 тис. дол. США.

Правоохоронним органом за матеріалами Держфінмоніторингу України ведеться досудове розслідування за ч. 3 ст. 209 "Легалізація (відмивання) доходів, одержаних злочинним шляхом" КК України.

Приклад

Громадянин М здійснював комп'ютерні атаки (DDoS) на інформаційні ресурси українських та зарубіжних комерційних структур. За допомогою спеціально модифікованого шкідливого програмного коду він створював бот-мережі (велику кількість інфікованих комп'ютерів).

Зокрема, для вчинення атак використовувалося програмне забезпечення "DirtJumperV5",

яке дозволяло віддалено керувати мережею з понад п'яти тисяч "зомбованих" (заражених) комп'ютерів, розташованих в різних країнах світу. Громадянин М з використанням бот-мереж вчинив понад 50 DDoS-атак.

Атаки проводилися на замовлення конкуруючих бізнес-структур.

Громадянин М приймав оплату за допомогою віртуальних платіжних систем (інтернет-гаманці були зареєстровані на підставних осіб). Для з'єднання з системою Інтернет на умовах передплати використовував радіомодеми.

Вироком суду за скоєння злочину, передбаченого ч. 1 ст. 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж: електрозв'язку" КК України, затриманого засуджено до сплати штрафу у розмірі 700 неоподаткованих мінімумів доходів громадян (11,9 тис. грн.), з конфіскацією програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання.

Приклад

В ході моніторингу мережі Інтернет правоохоронним органом виявлено факт розповсюдження фотозображень із сценами статевих актів за участю неповнолітнього хлопця.

Було проведено детальний аналіз фотозображень, в ході якого встановлено, що зображеного хлопця віком 8 - 12 років піддають сексуальному насильству дві дорослі особи.

В ході досудового розслідування вилучено понад 500 оптичних носіїв інформації із ексклюзивним контентом із змістом дитячої порнографії, 10 системних блоків, на жорстких дисках яких містяться аналогічні матеріали.

Двом особам, які здійснювали відеозйомки статевих актів з дітьми та в подальшому розповсюджували відзняті матеріали через глобальну мережу Інтернет, було пред'явлено обвинувачення за ч. 3 ст. 156 "Розбещення неповнолітніх", ч. 5 ст. 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів" КК України.

За результатом досудового слідства матеріали кримінальної справи були направлені до суду, яким винесено вирок у вигляді позбавлення волі на строки 9 та 11 років.

Приклад

В ході моніторингу мережі загального доступу Інтернет правоохоронним органом виявлено громадянина, який через різноманітні ресурси та форуми глобальної мережі рекламував та в подальшому реалізовував порно: фото-, відеоконтент у форматі "3D".

У ході проведення обшуку у помешканні вказаного вище громадянина виявлено та вилучено 5 одиниць комп'ютерної техніки, що використовувалася при вчиненні злочину.

За зібраними матеріалами було відкрито кримінальне провадження за ознаками складу злочину, передбаченого ст. 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів" КК України.

Особі оголошено повідомлення про підозру. Слідство триває.

Приклад

За зверненням правовласників щодо розповсюдження контенту в мережі Інтернет з

порушенням Закону України "Про авторське право та суміжні права" через веб-сайт "М" відкрито кримінальне провадження за ознаками складу злочину, передбаченого ч. 1 ст. 176 "Порушення авторського права і суміжних прав" КК України.

В ході досудового слідства встановлено осіб, які безпосередньо займалися наповненням контентом відповідного ресурсу та його рекламуванням через соціальні мережі та різноманітні форуми глобальної системи Інтернет.

У ході проведення слідчих дій вилучено 51 сервер із загальним обсягом інформації понад 400 терабайт, 13 одиниць комп'ютерної техніки та мережеве обладнання, а також кошти в сумі 61,5 тис. дол. США та 5,0 тис. грн.

Вартість вилученого обладнання за попередніми оцінками складає приблизно 1,5 млн. грн.

У ході слідства встановлено, що організатором діяльності даного ресурсу є іноземна компанія. Учасники компанії залучили громадянина Б як особу, яка здійснює на території України контроль за діяльністю ресурсу, залучає осіб для його технічної підтримки, а також відповідає за зв'язок з відвідувачами порталу.

Громадянину Б пред'явлено повідомлення про підозру. Рішенням суду щодо останнього обрано міру запобіжного заходу - особисте зобов'язання.

Приклад

Невстановленою особою здійснювалось блокування роботи телефонних номерів абонентів ПрАТ "Київстар", ПрАТ "Укртелеком" та ТОВ "ІнтерТелеком", які належать громадянці Б та використовуються нею для забезпечення роботи туристичної агенції.

Після перших годин блокування на персональний акаунт (Skype) громдянки Б надійшов лист з погрозою сплатити кошти в розмірі 1,2 тис. дол. США, інакше робота телефонів блокуватиметься невизначений час.

У ході слідства встановлено, що блокування роботи телефонних номерів агенції здійснювалося шляхом масового спрямування пакетів голосових даних ("SIP-пакетів") на зазначені вище телефонні номери.

Правоохоронним органом розпочато кримінальне провадження за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 356 "Самоправство" КК України.

3. ЛЕГАЛІЗАЦІЯ ДОХОДІВ, ОДЕРЖАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

На відміну від "традиційного" відмивання грошей, для здійснення якого використовується банківська система, кібервідмивання засноване на використанні різних видів операцій і постачальників фінансових послуг, починаючи з банківських переказів, внесення/зняття готівки, використання електронних грошей і закінчуючи "грошовими мулами" і послугами з переказу грошей.

Зазвичай ланцюжок переривається на операції з готівковими засобами, здійснювану як правило "грошовими мулами", за якою слідує використання традиційної платіжної системи. Якщо відповідний платіжний сервіс інтегрований з послугами з он-лайнових платежів, то гроші можуть бути переведені на електронні і без зволікання практично анонімно переведені в іншу державу.

Таким чином, виявлення і переслідування злочинних грошових потоків є дуже складним завданням для правоохоронних органів.

Такі заплутані схеми є викликом потужному, але традиційному програмному забезпеченню для збору даних у сфері протидії відмиванню доходів та фінансуванню тероризму, заснованому на поведінці клієнта, якщо частина "відмивального" ланцюжка реалізується абсолютно в іншій фінансовій ситуації.

Методи здійснення платежів в Інтернеті можуть також розділяти джерело, звідки надійшли інструкції на проведення операції, від реального місця проведення грошового переказу. Це є ще однією перешкодою для правоохоронних органів в частині виявлення і переслідування злочинних доходів.

3.1. Основні механізми легалізації злочинних доходів

Здобуті злочинним шляхом доходи вимагають від злочинців швидкого та ефективного проведення їх легалізації. При чому, з огляду на специфіку кіберзлочинності - організатори та виконавці схем переважно є освіченими та технічно грамотними, відповідно і методи, які ними використовуються при легалізації отриманих коштів, можуть також бути досить складними та нестандартними.

Інструменти та механізми, якими користуються злочинці під час здійснення відмивання доходів, одержаних у сфері кіберзлочинності, є досить різноманітними, зокрема при відмиванні доходів від кіберзлочинів характерним є використання наступних механізмів:

• використання рахунків, відкритих особами за втраченими документами, на підставних осіб;

• використання альтернативних платіжних систем (електронні платежі), як національних, так й міжнародних;

• проведення ланцюга фінансових операцій через декілька банківських рахунків за допомогою віддаленого доступу;

• використання готівки на останньому етапі ланцюга фінансових операцій;

• купівля електронних грошей та використання систем платежів через електронні гаманці;

• конвертація незаконних доходів у товари шляхом придбання останніх через мережу Інтернет.

Переведення викрадених коштів у готівку є поширеним, оскільки подальше переміщення готівки поза межами банківської системи майже неможливо відслідкувати. Широко практикується зняття готівки через банкомати з метою уникнення спілкування учасників схеми з працівниками банківських установ. В подальшому готівкові кошти через кур'єрів (грошових мулів) можуть бути безперешкодно передані анонімному організатору кіберзлочину.

Отримані злочинним шляхом кошти використовуються для покупки високоліквідних товарів або передплачених карток для подальшого їх перепродажу і отримання готівки. Також кошти можуть бути використані для придбання через Інтернет квитків, проїзних документів, предметів побуту та інших товарів для подальшого їх використання, перепродажу та отримання готівкових грошових коштів.

Частина злочинних доходів використовується на придбання нового обладнання та розробку більш ефективного шкідливого програмного забезпечення з тим, щоб обійти системи безпеки.

Слід зазначити також, що підставами для платежів, пов'язаних з несанкціонованим списанням коштів, можуть бути різноманітні призначення, які не дають можливості відокремлювати їх від інших фінансових операцій:

• оплата за ТМЦ (обладнання, прилади, нафтопродукти, металовироби, будматеріали, господарчі товари, офісні меблі, соняшник, олія соняшникова);

• оплата послуг (рекламно-поліграфічні послуги, роботи по контролю якості продукції, транспортно-експедиційне обслуговування, перевезення вантажу, проведення спортивних змагань);

• оплата по договору;

• надання/повернення фінансової допомоги (позики);

• поповнення карткового рахунку;

• сплата заробітної плати або відрядних;

• сплата за рішенням суду;

• повернення гарантійного внеску учаснику торгів за договором.

Водночас, іноді злочинці вказують підстави для зарахувань коштів з-за кордону й сумнівні призначення, зокрема виграш в казино, продаж прав інтелектуальної власності, продаж веб-сайтів або інтернет-магазинів, віртуальних казино тощо.

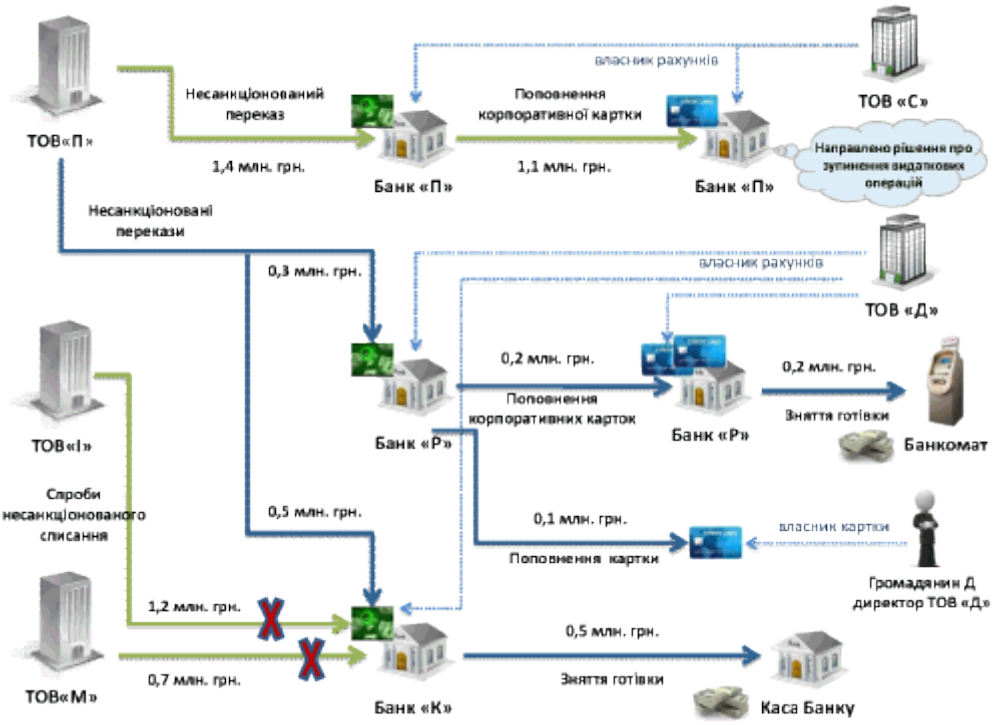
Приклад

Шляхом несанкціонованого доступу до рахунків юридичними особами "С" та "Д" здійснено заволодіння коштами ТОВ "П" за допомогою підроблення документів на переказ.

Грошові кошти, що надійшли на рахунок новоствореного ТОВ "С", в подальшому були перераховані на власний корпоративний рахунок. На підставі рішення Держфінмоніторингу України прийняті рішення про зупинення видаткових операцій по рахунках ТОВ "С".

Також з рахунку ТОВ "П" несанкціоновано списано кошти на рахунки ТОВ "Д". В подальшому кошти були зараховані на карткові рахунки та частково зняті готівкою у банкоматах.

Крім цього, здійснено спроби несанкціонованого перерахування коштів з рахунків ТОВ "М" та ТОВ "І" на рахунок ТОВ "Д" на підставі електронного платіжного доручення.



Рахунки ТОВ "С" та ТОВ "Д" відкриті незадовго до проведення фінансових операцій.

За вказаними фактами розпочато кримінальне провадження за ч. 4 ст. 190 "Шахрайство" КК України.

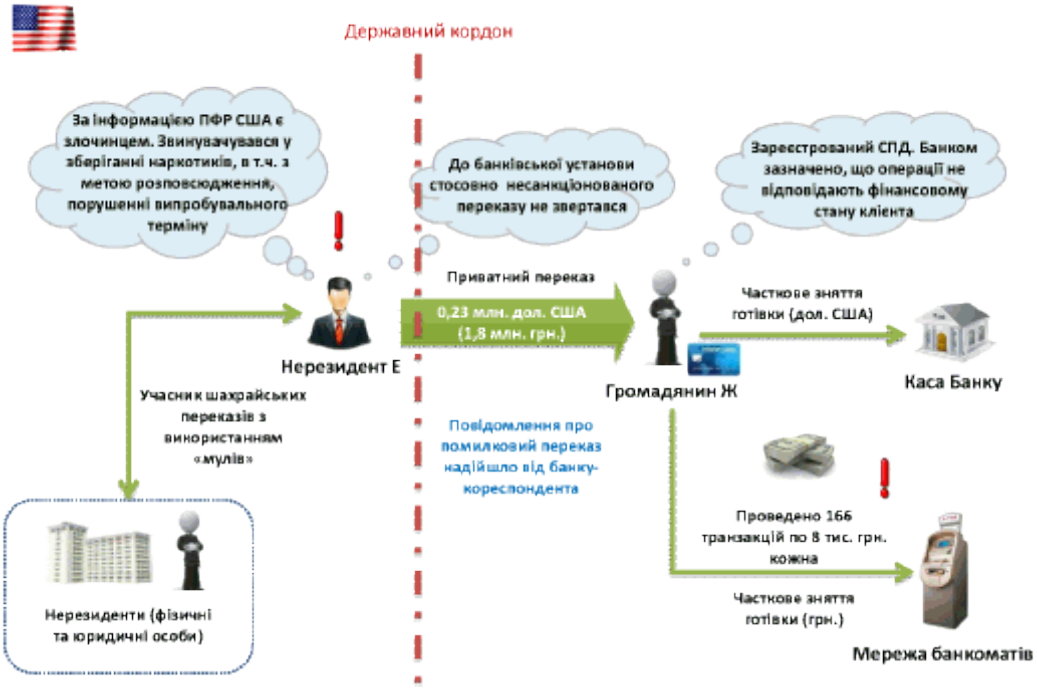
Приклад

Громадянином України отримано на власний картковий рахунок приватний переказ в сумі 0,23 млн. дол. США (1,8 млн. грн.) від фізичної особи - нерезидента з США.

Отримані кошти громадянином України в повному обсязі знято готівкою. При цьому частину коштів було знято через касу банку, а решту - значною кількістю транзакцій по 8,0 тис. грн. кожна через мережу банкоматів.

В подальшому від банку-кореспондента надійшов запит про помилковий переказ та прохання повернути кошти.

За інформацією ПФР США фізична особа - нерезидент є злочинцем. Він звинувачувався у зберіганні наркотиків, в т. ч. з метою розповсюдження, порушенні випробувального терміну.



Також було повідомлено, що зазначена особа є учасником шахрайських переказів за участю юридичних та фізичних осіб. Крім того, він причетний до схеми шахрайства з коштами з використанням "мулів" після прийняття пропозицій про роботу через Інтернет-сайт.

Слідство триває.

Приклад

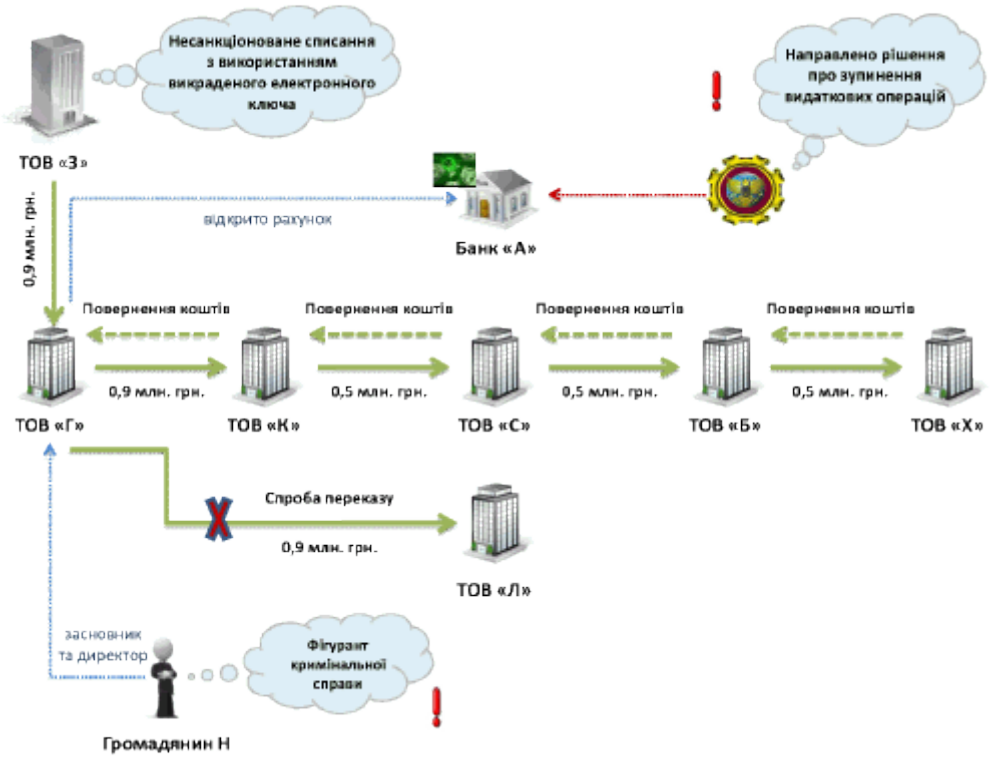
Виявлено факт несанкціонованого списання коштів з використанням викраденого електронного ключа у системі "Клієнт-Банк" в сумі 0,9 млн. грн. з поточного рахунку ТОВ "З" на користь ТОВ "Г".

Протягом одного дня викрадені кошти були перераховані транзитом через рахунки ряду підприємств.

В результаті своєчасно вжитих заходів кошти в повному обсязі повернулись на рахунок ТОВ "Г" та були заблоковані згідно рішення Держфінмоніторингу України.

Крім того, ТОВ "Г" здійснено спробу перерахування незаконно отриманих коштів на рахунок ТОВ "Л", однак банківською установою було відмовлено у проведенні зазначеної фінансової операції.

ТОВ "Г" - новостворене підприємство. Рахунок, на який надійшли викрадені кошти, відкрито за 10 днів до проведення вищезазначених операцій.



Директор та засновник ТОВ "Г" - громадянин Н - є фігурантом кримінальної справи за ч. 1 ст. 191 "Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем" КК України.

Приклад

Виявлено несанкціоновані перекази від значної кількості підприємств на рахунки ФОП "Ш", відкриті у банках "А" та "Б".

Привертає увагу, що списання з рахунків чотирьох підприємств на рахунок ФОП "Ш" у банку "А" відбувалось протягом одного дня. В подальшому частину коштів ФОП "Ш" було знято з рахунку готівкою.

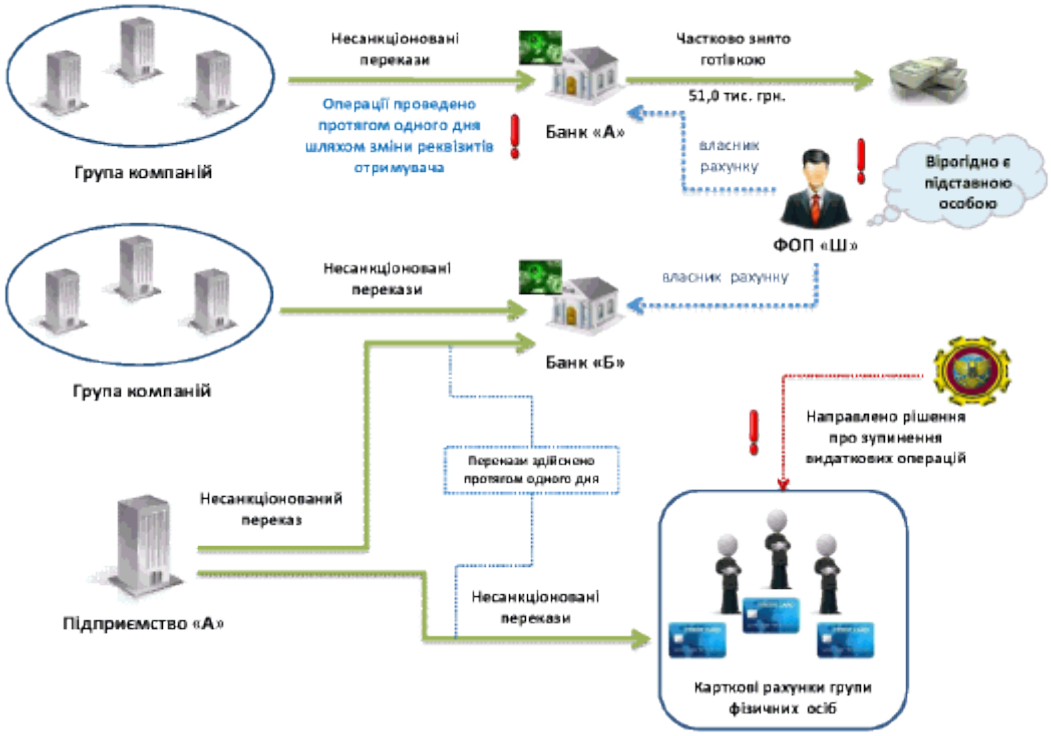
Шахрайські перекази було здійснено шляхом втручання в роботу системи "Клієнт-Банк" та зміни реквізитів отримувача.

За наявною інформацією ФОП "Ш" вірогідно є підставною особою та веде антисоціальний спосіб життя.

Крім того, на рахунок ФОП "Ш" у банку "Б" було здійснено несанкціонований переказ з рахунку підприємства "А" у сумі 280,0 тис. грн. Того ж дня кошти було повернуто відправнику.

В цей же день з рахунку підприємства "А" було здійснено несанкціоновані перекази на карткові рахунки семи громадян України.

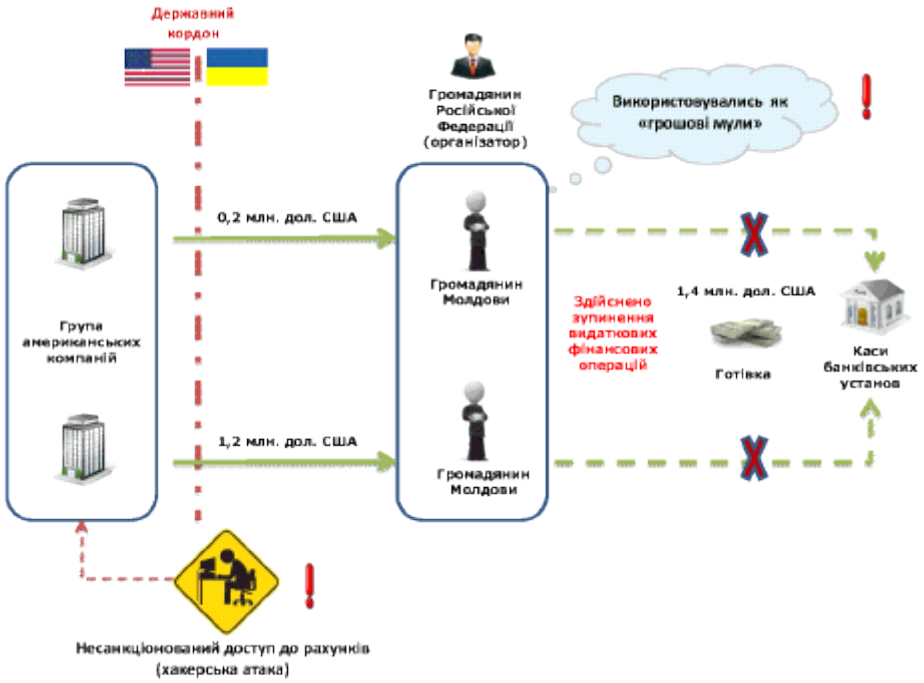
Держфінмоніторингом України прийнято рішення щодо зупинення фінансових операцій по рахунках зазначених громадянин України.



За вказаними фактами розпочато кримінальне провадження за ч. 4 ст. 190 "Шахрайство" КК України.

Приклад

Правоохоронним органом за матеріалами Держфінмоніторингу України встановлено групу з трьох учасників у складі росіянина та двох молдован, причетних до легалізації на території України коштів американських компаній, отриманих внаслідок їх незаконного заволодіння, шляхом здійснення несанкціонованого доступу до рахунків цих компаній.



Спочатку реалізації такої схеми злочинцями викрадено 1,4 млн. дол. США (еквівалент 11,1 млн. грн.). Дані кошти надійшли на рахунки зазначених осіб, відкриті в українських банках. Підставою для отримання коштів громадяни Молдови вказували фінансову допомогу, однак довіреною особою при спробі зняття грошових коштів джерелом їх надходження зазначено дохід від продажу інтернет-казино.

Вказана розбіжність у поясненнях власників рахунків та уповноваженої особи стала підставою для зупинення видаткових операцій по рахунках банківською установою. В подальшому банківські рахунки заблоковано Держфінмоніторингом України та правоохоронним органом на них накладено арешт.

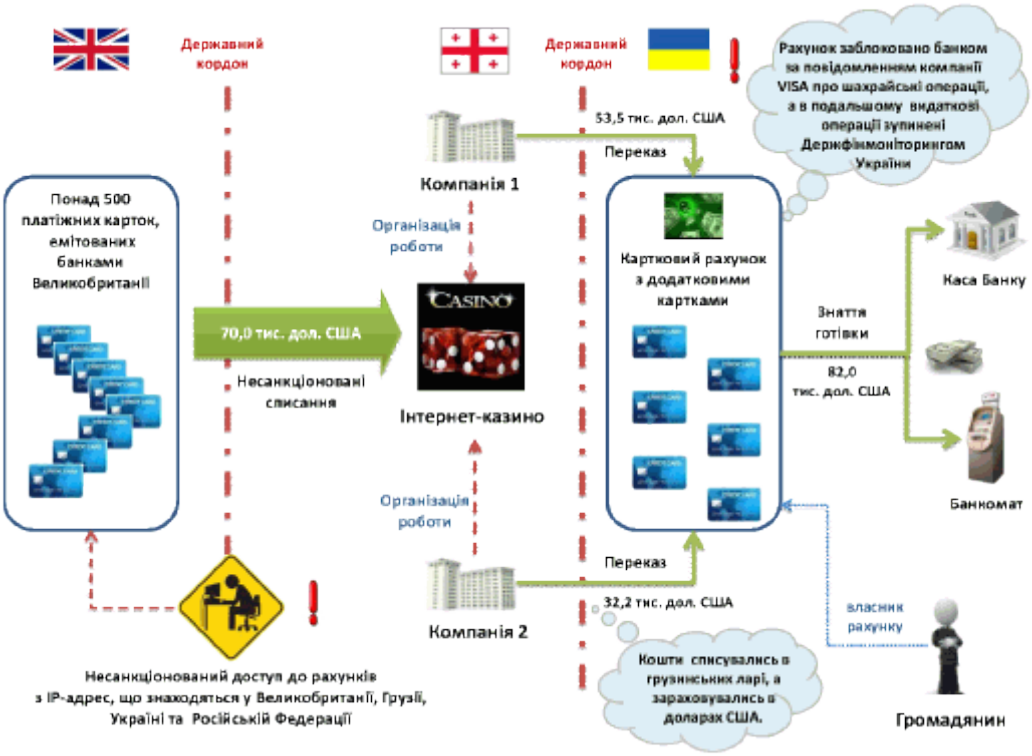
За даною справою судом першої інстанції оголошено вирок, яким засуджено росіянина-організатора злочину на 10 років позбавлення волі, прийнято рішення про конфіскацію майна, відносно двох молдован прийнято рішення щодо позбавлення волі на менші строки.

Приклад

На картковий рахунок громадянина України зараховано перекази в загальній сумі 85,7 тис. дол. США від двох грузинських компаній - операторів електронних ігор, які обслуговують діяльність інтернет-казино.

Компанією VISA було повідомлено український банк про те, що джерелом походження коштів були несанкціоновані списання з платіжних карток, емітованих банками Великобританії, через інтернет-казино. Загальна кількість карток - понад 500, а сума завданих збитків - близько 70,0 тис. дол. США.

Несанкціонований доступ відбувався з IP-адрес, розташованих у Великобританії, Грузії, Україні та Російській Федерації.



В подальшому громадянин України отримані кошти знімав готівкою через касу банку та банкомати і витрачав на власні потреби.

Держфінмоніторингом України прийнято рішення щодо зупинення видаткових фінансових операцій.

Правоохоронним органом проводиться розслідування.

Приклад

Групою громадян організовано мережу спеціалізованих ігрових залів закритого типу з надання послуг грального бізнесу населенню, а саме доступ до азартних ігор на комп'ютерних носіях через мережу Інтернет.

За результатами діяльності такого інтернет-бізнесу одним з організаторів одержано дохід в сумі понад 1,0 млн. грн.

З метою легалізації незаконного доходу вказаною особою кошти направлено на придбання виробів із дорогоцінних металів та подальшого розміщення для зберігання, відповідно до договорів на користування індивідуальними сейфами в сховищах комерційних банків.

За матеріалами правоохоронного органу відкрито кримінальне провадження за ч. 1 ст. 203^2 "Зайняття гральним бізнесом" КК України за фактом виявлення підпільних гральних закладів.

За результатами проведення обшуків в приміщеннях гральних закладів, офісу та за місцями проживання фігурантів вилучено 317,0 тис. грн., 19,8 тис. дол. США, 7,1 тис. євро, 56 одиниць гральних автоматів, 526 - комп'ютерної техніки (системні блоки, монітори, ноутбуки, модеми), 57 мобільних телефонів, 2 електронні рулетки, пістолет з ознаками переробки системи "Наган" з глушником та набої до нього калібром 9-мм в кількості 15 шт.

В ході розслідування відкрито кримінальне провадження за ч. 2 ст. 209 "Легалізація (відмивання) доходів, одержаних злочинним шляхом" КК України відносно одного з організаторів незаконної діяльності.

Приклад

Громадянка Л, займаючи посаду провідного експерта Банку, шляхом обману та зловживання довірою, використовуючи електронно-обчислювальну техніку, а саме встановлений на її робочому місці та приєднаний до мережі системи "Клієнт-Банк" комп'ютер, заволоділа коштами, які знаходились на рахунку громадянина Ш.

Будучи обізнаною про незаконне походження коштів з метою маскування незаконного їх походження, громадянка Л перерахувала кошти на розрахунковий рахунок свого чоловіка.

Кошти, одержані злочинним шляхом, громадянка Л використала з метою збільшення спільного сімейного бюджету, отримання та оплати спільних побутових благ, придбання товарів та послуг, а також надання можливості використання даних коштів її чоловіком у його підприємницькій діяльності.

Громадянка Л вчинила легалізацію коштів, одержаних злочинним шляхом, на загальну суму 307,1 тис. грн.

З метою забезпечення відшкодування завданих збитків правоохоронним органом накладено арешт на майно на загальну суму 200,0 тис. грн.

В результаті проведених заходів відшкодовано збитків на суму 123,6 тис. грн.

Відповідно до вироку суду громадянку Л визнано винною у скоєнні злочинів, передбачених ч. 3 ст. 190 "Шахрайство", ч. 1, ч. 2 ст. 209 "Легалізація (відмивання) доходів, одержаних злочинним шляхом" КК України, і призначено покарання у вигляді позбавлення волі на 5 років з позбавленням права обіймати посади, пов'язані з обслуговуванням грошових коштів у кредитно-фінансових установах, на 3 роки з конфіскацією коштів в сумі 307,1 тис. грн., одержаних злочинним шляхом.

3.2. Використання альтернативних платіжних систем для відмивання доходів

З метою зручного та швидкого переказу коштів, одержаних у сфері кіберзлочинності, злочинцями широко використовуються можливості платіжних систем або систем переказу коштів.

Законодавство України передбачає діяльність в Україні внутрішньодержавних та міжнародних платіжних систем.

Внутрішньодержавна платіжна система - платіжна система, в якій платіжна організація є резидентом та яка здійснює свою діяльність і забезпечує проведення переказу коштів виключно в межах України.

Міжнародна платіжна система - платіжна система, в якій платіжна організація може бути як резидентом, так і нерезидентом і яка здійснює свою діяльність на території двох і більше країн та забезпечує проведення переказу коштів у межах цієї платіжної системи, у тому числі з однієї країни в іншу.

За інформацією Національного банку України, за станом на 01.07.2013 на території України здійснювали діяльність з переказу коштів дев'ять внутрішньодержавних і міжнародних систем переказу коштів, створених резидентами України, із яких п'ять систем

запроваджені банками та чотири системи - небанківськими установами України.

Також на території України функціонують 22 міжнародні системи переказу коштів, створені нерезидентами. Учасниками таких систем є більше 150 банків України, ПрАТ "Українська фінансова група" та національний оператор поштового зв'язку УДППЗ "Укрпошта".

У І півріччі 2013 року з використанням внутрішньодержавних та міжнародних систем переказу коштів, створених як резидентами, так і нерезидентами, було переказано:

• у межах України - 7915,0 млн. грн. та 4,5 млн. дол. США (в еквіваленті);

• в Україну - 2203,0 млн. дол. США (в еквіваленті);

• за межі України - 384,0 млн. дол. США (в еквіваленті).

Платіжні системи мають ряд незаперечних переваг, які і обумовлюють їх швидкий розвиток, а саме:

• доступність - відкриття власного електронного рахунку є безкоштовним для будь-якого користувача;

• простота використання - відкриття та використання електронного рахунку є інтуїтивно зрозумілим і не потребує спеціальних знань;

• мобільність - користувач через мережу Інтернет може здійснювати управління своїм рахунком з будь-якого місця;

• оперативність - транзакції по рахунку відбуваються протягом декількох секунд;

• безпека - передача інформації ведеться з використанням криптографічного захисту.

Щоб стати учасником і користуватися послугами платіжної системи потрібно пройти процес реєстрації й відкрити в ній електронний рахунок у вигляді електронного гаманця. Електронний гаманець зберігає інформацію про суму коштів на рахунку користувача в платіжній системі.

Для проведення фінансових операцій необхідно ввести гроші в платіжну систему, тобто поповнити електронний рахунок. Різні платіжні системи пропонують різні способи поповнення електронних гаманців. Це може бути банківський переказ, поштовий переказ, придбання передплаченої картки, поповнення через платіжний термінал та ін.

Крім того, для переміщення готівкових коштів між учасниками схеми можуть використовуватись термінові перекази через міжнародні системи переказу коштів.

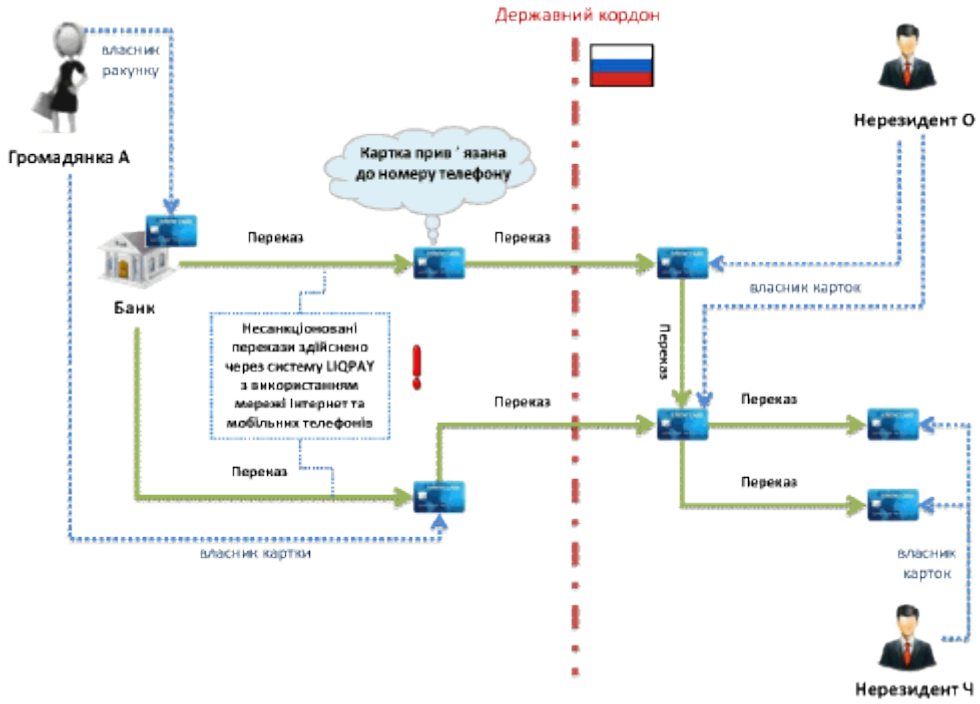
Механізм таких переказів є досить простим та зручним. Для цього у відділення системи або її партнера звертається особа (необхідно мати документ, що засвідчує особу), яка вносить необхідні кошти та заповнює бланк із зазначенням прізвища та ім'я отримувача і країни відправлення переказу. В подальшому від оператора отримується номер переказу, який необхідно повідомити отримувачу.

Отримувач коштів (з документом, що засвідчує особу) звертається до відділення системи або її партнера та заповнює бланк на видачу готівки із зазначенням номеру переказу, прізвища та ім'я відправника, країни відправлення переказу, суми та валюти переказу.

Здійснення переказу та отримання готівки займає лише декілька хвилин.

Приклад

З карткового рахунку громадянки України здійснено несанкціоноване списання коштів.



В результаті здійснення ряду несанкціонованих переказів кошти зараховано на карткові рахунки двох громадян Російської Федерації.

Перекази здійснено за допомогою електронної платіжної системи LIQPAY з використанням мережі Інтернет та доступу через мобільні телефони.

Правоохоронним органом розпочато кримінальне провадження за ч. 1, 2 ст. 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку" та ч. 3 ст. 190 "Шахрайство" КК України.

Приклад

Члени кіберзлочинного угрупування у складі 11 осіб (у т. ч. громадян України) - продали більш як 95 тисяч номерів крадених кредитних карток через мережу Інтернет.

Загальна сума збитків, завданих цим злочином, склала 5,0 млн. дол. США.

Для відмивання та переказу незаконно одержаних коштів від продажу платіжних карток шахраї використали платіжну систему "Western Express International".

Прокуратурою Манхеттена м. Нью Йорк, США, оголошено про те, що винесені всі вироки у кримінальній справі про торгівлю номерами десятків тисяч крадених кредитних карт і особистих даних.

До відповідальності притягнуто 17 осіб різних країн світу, у тому числі Росії та України. Справа розслідувалася 8 років.

Відповідно до звинувачення у продажу 75 тисяч карт з цього числа звинувачують

громадянина України.

Судом винесено вирок стосовно нього про відбування покарання строком 13 років і 4 місяці у в'язниці.

3.3. Використання електронних грошей для відмивання доходів

За законодавством України електронні гроші - це одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими, ніж емітент, особами і є грошовим зобов'язанням емітента. Випуск електронних грошей в Україні мають право здійснювати лише банки (емітенти). Емітенти мають право здійснювати випуск електронних грошей, виражених лише в гривнях.

Сума електронних грошей на електронному пристрої, який не може поповнюватися, не повинна перевищувати 2 тис. грн. Сума електронних грошей на електронному пристрої, який може поповнюватися, не повинна перевищувати 8 тис. грн.

Погашення електронних грошей, пред'явлених користувачами - фізичними особами, може здійснюватись готівковими коштами або шляхом переказу на банківський рахунок пред'явника. Погашення електронних грошей, пред'явлених користувачами - суб'єктами господарювання, торговцями, агентами, емітент зобов'язаний здійснювати виключно шляхом переказу на їх банківські рахунки.

За допомогою електронних грошей можливо здійснювати наступні платежі:

• платежі в середині системи на рахунки фізичних та юридичних осіб;

• оплата товарів в Інтернет-магазинах;

• оплата послуг операторів мобільного зв'язку;

• оплата комунальних послуг;

• оплата Інтернет-послуг;

• оплата державних зборів, мита та штрафів;

• купівля ж/д та авіаквитків;

• купівля палива та замовлення паливних скретч-карт;

• бронювання готелів та ін.

Для злочинців безперечною перевагою використання електронних грошей є можливість анонімного відкриття та поповнення електронних гаманців, а також цілодобова доступність та швидкість проведення транзакцій (протягом декількох секунд). Електронний гаманець фізичної особи найчастіше має прив'язку до електронної пошти або номеру мобільного телефону.

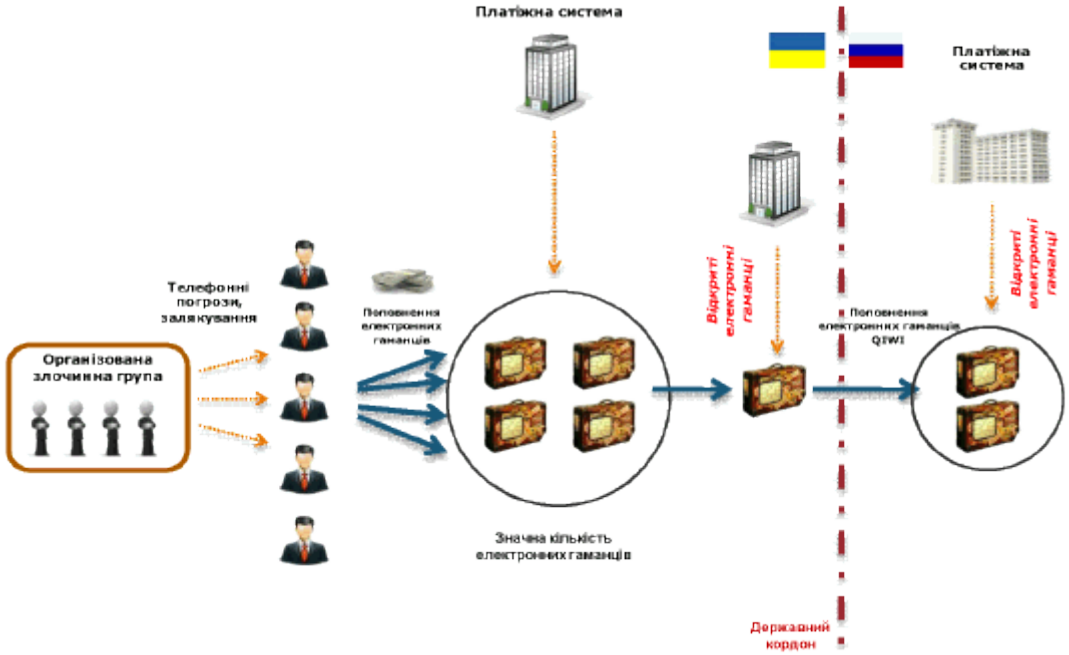
Приклад

Організована злочинна група, шляхом телефонних погроз та залякування, шантажуючи здоров'ям та безпекою родичів, примушувала фізичних осіб до поповнення електронних гаманців, які їм не відомі.

На електронні гаманці, відкриті у платіжній системі, заляканими фізичними особами внесено кошти загальній сумі 30,0 тис. грн.

В подальшому, з метою легалізації вищевказаних коштів, з зазначених електронних гаманців здійснені перекази на інші платіжні системи.

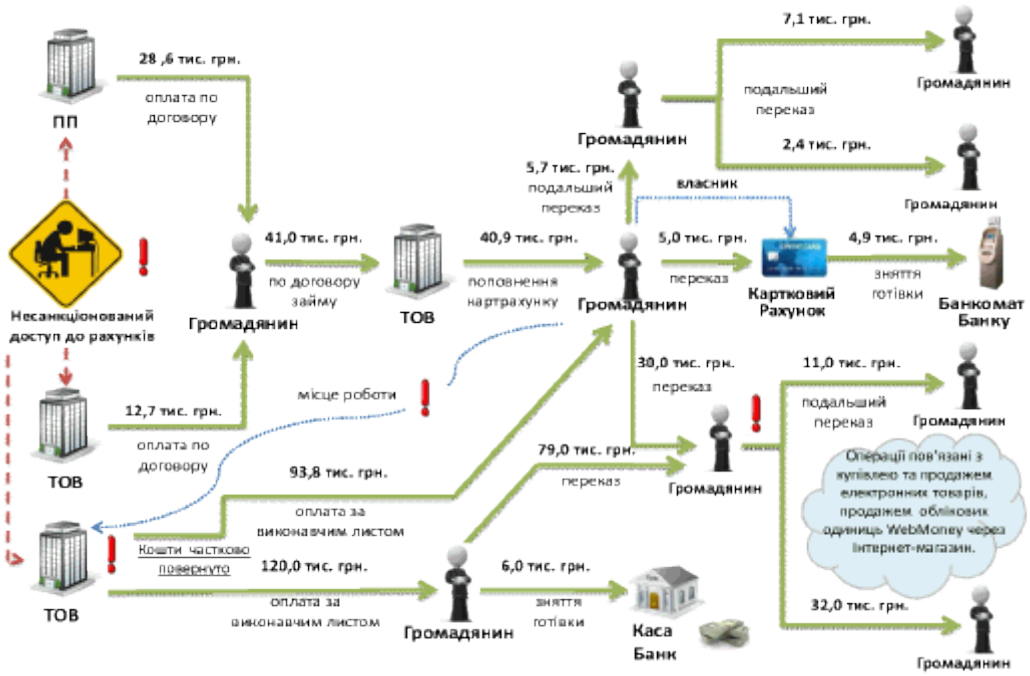
Електронні кошти були призначені для обміну на безготівкові кошти та подальшого переказу для поповнення електронних гаманців міжнародної платіжної системи (Російська Федерація).



Правоохоронним органом за матеріалами Держфінмоніторингу України ведеться розслідування.

Приклад.

Трьома фізичними особами організовано та вчинено шахрайські дії з несанкціонованого списання грошових коштів з рахунків юридичних осіб з віддаленим керуванням ними із використанням новітніх інформаційних технологій.



Несанкціоновано списані грошові кошти з рахунків 3 юридичних осіб, які зареєстровані в різних регіонах України, перераховані транзитом через рахунки фізичних осіб, та зараховані на карткові рахунки третіх фізичних осіб.

В подальшому, частина коштів конвертована в "електронні гроші" та знята готівкою.

Правоохоронним органом за матеріалами Держфінмоніторингу України ведеться досудове розслідування за ч. 3 ст. 209 КК України "Легалізація (відмивання) доходів, одержаних злочинним шляхом".

Приклад

Встановлено, що фізична особа - підприємець, за попередньою змовою з двома фізичними особами та діючи в порушення чинного законодавства України, у період 2011 - 2013 рр., застосовували та використовували у фінансово-господарської діяльності електронні гроші, емітовані незареєстрованими платіжними системами.

Вказані особи надавали послуги з вводу/виводу, обміну, конвертації (переведення у готівку та навпаки) електронних грошей (українська гривня, долар США, євро, російський рубль) за допомогою зазначених платіжних систем.

За фактом здійснення фінансових операцій з коштами, одержаними внаслідок вчинення суспільно небезпечного протиправного діяння, що передувало легалізації (відмиванню) доходів у великому розмірі розпочато кримінальне провадження, що кваліфікується за ст. 209 "Легалізація (відмивання) доходів, одержаних злочинним шляхом" КК України (предикатом виступає ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення" КК України), та три кримінальних провадженнях, що кваліфікуються за ст. 212 "Ухилення від сплати податків, зборів (обов'язкових платежів)" КК України.

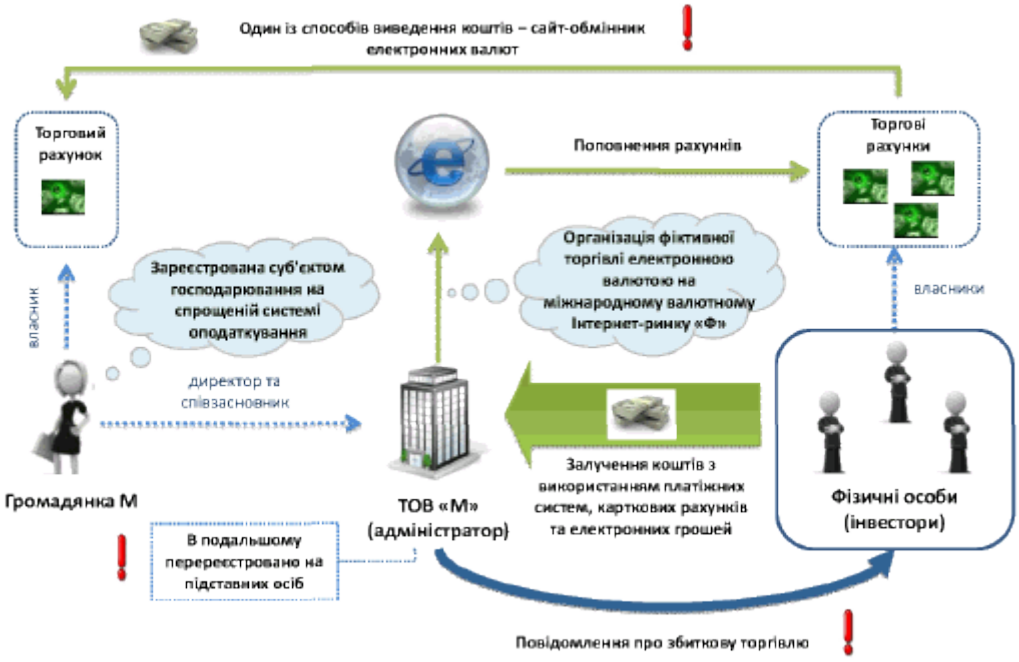
На даний час досудове розслідування триває.

Приклад

Громадянкою М, яка знаходиться на спрощеній системі оподаткування та одночасно являється генеральним директором і співзасновником ТОВ "М", організовано залучення грошових коштів фізичних осіб - інвесторів для здійснення торгівлі електронною валютою на міжнародному валютному Інтернет-ринку "Ф".

Грошові кошти отримуються шахрайським шляхом від фізичних осіб з використанням платіжних систем, переказів через карткові рахунки, переказів з використанням електронних грошей.

Для забезпечення залучення клієнтів-інвесторів та здійснення контролю за отриманими доходами було створено низку сайтів.



Клієнтами-інвесторами внесено власні готівкові кошти для участі в торговій операціях на міжнародному валютному Інтернет-ринку "Ф". При цьому, ТОВ "М" укладено угоди громадянами України, згідно яких ТОВ "М" було адміністратором, а фізичні особи - інвесторами.

Після цього, організатори схеми надавали логін та пароль інвесторам для доступу до "особистих кабінетів" сайтів, підконтрольних організаторам.

Фізичним особам - інвесторам повідомлялось, що готівка переводиться на їх особисті рахунки на платформі визначеного програмного забезпечення для подальшої участі в проведенні торгів на ринку "Ф".

Фізичні особи деякий час бачили в "особистих кабінетах" сайтів участь своїх інвестованих коштів у торгових операціях на ринку "Ф".

Однак, через деякий час надходила інформація щодо відсутності на рахунках коштів. При зверненні інвесторів до адміністраторів щодо причини зникнення коштів останнім надавалися пояснення, що грошові кошти було втрачено внаслідок здійснення неприбуткової операції.

Через деякий час ТОВ "М" перереєстровано на підставних осіб, торгові рахунки клієнтів закриті.

При цьому штучно створені умови для "злиття" торгових рахунків більшості клієнтів-інвесторів - втрати ними всіх вкладень за рахунок неприбуткової торгівлі.

Одним зі способів введення-виведення грошових коштів на торгові рахунки громадянки М є сайт - обмінник електронних валют, власником якого є громадянин Л, який знаходиться на спрощеній системі оподаткування.

Для приховування обсягів грошових коштів, що конвертуються через сайт-обмінник, громадянином Л використано банківські карткові та віртуальні рахунки, про відкриття яких не повідомляється органам Міністерства доходів та зборів України.

Передача грошових коштів між СГД - фіктивними особами здійснюється переказами на карткові рахунки та безпосередньою передачею готівки.

За результатами проведених заходів розпочато кримінальне провадження за ознаками злочинів, передбачених ч. 3 ст. 190 "Шахрайство" та ч. 1 ст. 209 "Легалізація (відмивання) доходів, одержаних злочинним шляхом" КК України.

4. СПОСОБИ ТА МЕТОДИ ПОПЕРЕДЖЕННЯ ТА ПРОТИДІЇ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОДЕРЖАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

4.1. Загальні напрямки протидії кіберзлочинам

Надзвичайно швидкий розвиток інформаційних та комп'ютерних технологій останнім часом призводить до стрімкого розвитку кіберзлочинності, тому особливої актуальності сьогодні набувають питання попередження та протидії злочинам у кіберпросторі.

Попередження кіберзлочинності базується на заходах, спрямованих на зниження ризику здійснення таких злочинів та нейтралізацію шкідливих наслідків для суспільства та приватного сектору.

Ефективна протидія кіберзлочинам повинна поєднувати комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів.

На законодавчому рівні в Україні залишається невирішеними чимало питань у сфері протидії кіберзлочинності. Це, насамперед, відсутність у вітчизняному законодавстві чіткого визначення поняття "кіберзлочинність". Визначення такого терміну може дати значний поштовх до приведення у відповідність інших законодавчих актів.

Вдосконаленню законодавчого та нормативно-правового забезпечення у сфері попередження та протидії легалізації доходів, пов'язаних із злочинами у сфері кіберзлочинності, можливе за наступними напрямами:

• внесення змін до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій;

• визнання електронних документів та інших даних у якості доказової бази при розслідуванні кіберзлочинів;

• чітка регламентація механізмів взаємодії між клієнтом та банком, між банком

відправника коштів та банком отримувача коштів у разі несанкціонованого списання коштів клієнта (шляхом внесення змін до Інструкції про безготівкові розрахунки в Україні в національній валюті);

• запровадження практики ідентифікації користувача Інтернет шляхом надання ідентифікаційного коду особи оператору зв'язку, при подачі письмової заяви про укладення договору на надання послуг;

• закріплення вимоги щодо обов'язкового проведення двоканальної аутентифікації та обов'язкового online-інформування клієнтів про кожну проведену операцію;

• обов'язку банків безкоштовно в обов'язковому порядку підключати послугу СМС інформування у частині здійснення будь-яких операцій за поточними картковими рахунками;

• обов'язку банків щодо можливості проведення вихідних платежів клієнтів тільки за рахунок залишків на їх рахунках на початок операційного дня. У такому випадку банк, в якому відбулось несанкціоноване списання коштів, та клієнт, що постраждав, будуть мати додатковий час для можливості блокування коштів на рахунку недобросовісного отримувача;

• введення сертифікації електронних платіжних засобів;

• встановлення фіксованого максимального розміру видачі готівки, яка може проводитись в позаопераційний час банку по одному картковому рахунку через банкомат і який неможливо змінювати;

• обов'язку банків встановити антискімингові пристрої на всіх банкоматах;

• впровадити реєстрацію в податкових органах Інтернет-магазинів відносно конкретних платників податків.

З метою попередження кіберзлочинів банківськими установами можуть впроваджуватись наступні технічні та організаційні заходи:

• періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв;

• впровадження для клієнтів банку карток з мікропроцесором (чіпом), як більш захищених від підробки;

• ведення "чорного" списку рахунків (кодів ЄДРПОУ, ДРФО, IP-адрес) шахраїв для своєчасного блокування операцій;

• вимоги щодо двофакторної/двоканальної аутентифікації;

• використання токенів для зберігання електронних цифрових підписів користувачів;

• обов'язкове інформування клієнтів про кожну проведену операцію;

• підтвердження платежу в телефонному режимі;

• генерація клієнтського ключа самим клієнтом, що унеможливлює вчинення неправомірних дій зі сторони працівників банку;

• прив'язка ключа клієнта до серійного номеру жорсткого диску / флеш накопичувача / дискети, що унеможливлює копіювання ключів Клієнт-Банку та доступ до сторінки клієнта за допомогою інших комп'ютерів;

• використання ряду логічних правил для типових/нетипових/підозрілих платежів в

системі Клієнт-Банк;

• використання клієнтом окремого комп'ютеру, який призначений тільки для системи Клієнт-Банк (інтернет-банкінг), з налаштованими міжмережевими фільтрами;

• статистичний аналіз трафіку (Netflow) для виявлення аномалій;

• встановлення лімітів на проведення операцій у мережі Інтернет;

• встановлення лімітів на проведення операцій у певних ризикових країнах;

• встановлення лімітів на проведення операцій за їх періодичністю.

Слід зазначити, що значна частина кіберзлочинів стає можливою завдяки необізнаності населення та недотриманню основних правил безпеки. Такими чинниками, зокрема, є:

• обмежена кількість даних та інформації про кіберзлочини;

• низький рівень обізнаності щодо ризиків, спричинених впровадженням нових платіжних систем та сервісів, а також щодо пов'язаного з ними відмивання коштів;

• встановлення та використання неліцензійного програмного забезпечення (операційні системи, антивіруси тощо);

• ненадійне зберігання електронного цифрового підпису та кодів доступу (паролів) клієнтами банківських установ;

• нехтування елементарними правилами безпеки при користуванні Інтернет-банкінгом та спеціальними платіжними засобами в мережі Інтернет;

• невиконання політики кодової (парольної) та інформаційної безпеки.

В зв'язку з цим значну користь у попередженні кіберзлочинності мають інформаційно-просвітницькі заходи щодо нових ризиків та загроз в інформаційних та комп'ютерних системах.

Національним банком України з метою попередження шахрайства з платіжними картками розроблено Рекомендації держателям платіжних карток щодо їх використання, які розміщені на сторінці офіційного представництва Національного банку України в мережі Інтернет у розділі "Платіжна система" (http://wvyw.bank.gov.ua/doccatalog/document?id=70904Y).

4.2. Виявлення підозрілих фінансових операцій, що можуть бути пов'язані з відмиванням доходів, одержаних у сфері кіберзлочинності

Незважаючи на досвідченість кіберзлочинців та використання ними широкого інструментарію схем для легалізації незаконних доходів, представляється можливим виділити фінансові операцій за рівнем ризику.

Більше того, можливо також визначити сфери та послуги, які мають підвищений ризик та відповідно потребують підвищеної уваги.

Індикаторами підозрілості фінансових операцій зазначеної спрямованості для банківських установ опосередковано можуть бути наступні фактори:

• спроба входу із забороненого/нового IP-адресу;

• спроба використання прострочених первинних/робочих або старих ключів після

сертифікації нових;

• використання для банківських операцій IP-адрес та імен користувачів, за якими попередній моніторинг виявив причетність до шахрайських операцій;

• трансакції в нестандартний час або підключення до системи у вечірній час;

• незвичайні умови або складність операції: висока частота переказів коштів протягом невеликого періоду часу, велика кількість різноманітних джерел походження коштів та платіжних методів (інструментів);

• особа не інформована про характер діяльності юридичної особи, яку вона представляє;

• особа не може пояснити необхідність надання тієї або іншої банківської послуги;

• залучення до проведення операцій осіб молодого віку та/або новостворених підприємств;

• проведення операцій за втраченими документами;

• відкриття рахунку, на який зараховуються кошти внаслідок несанкціонованого списання, незадовго до проведення таких операцій;

• спроби зняти кошти в день їх зарахування;

• намагання клієнта отримати дві або більше банківських карток, що не відповідає суті його діяльності або обороту;

• зарахування коштів на карткові рахунки фізичних осіб з подальшим зняттям через банкомата (в т. ч. інших банків);

• операції не відповідають попереднім операціям клієнта;

• відсутність інформації щодо господарської діяльності клієнта або використання он-лайнових платіжних систем замість традиційних;

• міжнародні перекази, які отримуються / перераховуються з / за кордон, що не відповідає діяльності клієнта.

ВИСНОВКИ

Незважаючи на відсутність на сьогодні загальноприйнятного визначення кіберзлочину, спостерігається досить широке та вичерпне розуміння його суті та способів його вчинення, а також загроз та ризиків, що дає можливість розробляти та запроваджувати заходи протидії даному виду злочину.

Відсутність фізичного контакту з жертвою або представниками фінансової установи, а також анонімність, швидкість здійснення та невисока вартість злочину стали ключовими передумовами підвищення зацікавленості злочинців кіберпростором.

Інтернет-простір став не тільки місцем вчинення злочину та одержання незаконного доходу, а й місцем легалізації такого доходу. При цьому різноманіття видів кіберзлочинів у сукупності з різноманіттям способів відмивання доходів, одержаних від скоєння даних видів злочинів, призводять до складності їх виявлення та розслідування.

Виявлені схеми та механізми відмивання доходів, одержаних від кіберзлочинності, дозволяють стверджувати, що переміщення коштів можливе як традиційними способами

переказу, так і з використанням сучасних систем термінових переказів, електронних платіжних систем та електронних грошей.

При цьому, кошти використовуються в одних випадках для придбання передплачених карток, товарів або послуг в мережі Інтернет, а в інших переводяться у ігрові фішки казино або електронні гроші та перераховуються між електронними гаманцями, з подальшим переведенням у готівку.

В свою чергу, використання готівки залишається одним з найбільш розповсюджених та ефективних способів приховування як подальшого руху незаконного доходу та напрямків його вкладення, так й джерел походження таких коштів під час введення коштів до банківської системи. Це дозволяє злочинцям підтримувати подальшу анонімність, здобуту на етапі одержання незаконного доходу й під час відмивання доходів.

Протидія кіберзлочинам поєднує комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів, при цьому роль кожного з цих заходів не може бути визначена пріоритетною чи другорядною. При цьому ефективна протидія відмиванню злочинних доходів та зниження рівня злочинності в цій сфері можливі завдяки своєчасному виявленню фінансових операцій, що можуть бути пов'язані з відмивання доходів, одержаних у сфері кіберзлочинності, та ефективному співробітництву між державним та приватним сектором.