Тернопільський національний економічний університет

Юридичний факультет

Кафедра фінансово-економічної безпеки та інтелектуальної власності

МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА

на тему:

«ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ»

Студента 1 курсу магістратури
групи ФЕБм - 11
Галузі знань 1801 – специфічні категорії
Спеціальності 8.18010014 “Управління фінансово-економічною безпекою”
Скалюка Ю.О.

Керівник _____
_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____Оцінка: ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали

м. Тернопіль – 2016 рік

ЗМІСТ

ВСТУП

Модерне суспільство – це суспільство інформаційних технологій, що ґрунтується на щоденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів спілкування та інших технічних засобів. Поточна робота державних структур, транспортної, енергетичної, банківської та інших систем нездійснима без безпечної роботи комп'ютерної техніки та способів комунікацій.

Інформаційні технології стали стабільним супутником сьогочасної людини не тільки на робочому місці, вони проникнули майже в усі сфери людського життя. Поширення сучасних інформаційних технологій, в основі яких лежить широке вживання комп'ютерної техніки та способів комунікацій, автоматизації та оптимізації процесів в усіх без виключення галузях життєдіяльності, спричинило до нівелювання меж та переплетення національних господарств та національних інфраструктур країн світу.

Банківська система України є однією з галузей, де найбільш широко та активно використовуються новітні можливості інформаційних технологій та мережі Інтернет. А зважаючи, що зазначені технології використовуються для грошових переказів, вказана сфера привертає все більшу увагу злочинців.

Несанкціоноване списання грошових коштів з банківських рахунків, розповсюдження комп'ютерних вірусів, шахрайство з платіжними картками, DDoS атаки на Інтернет-ресурси, втручання в роботу Інтернет-банкінгу, шахрайство в інформаційних мережах – це не повний перелік кіберзлочинів, тобто злочинів у галузі комп'ютерних та інформаційних технологій.

Актуальність теми дослідження полягає у відсутності чіткої та злагодженої системи заходів для вчасного виявлення фінансових операцій, що можуть бути пов'язані з відмиванням доходів, отриманих у галузі кіберзлочинності в Україні.

Вищевказані прерогативи даного виду злочину поряд з його значною прибутковістю стали безсумнівно істотними перевагами у порівнянні з іншими

злочинами, скоєння яких в умовах покращання правоохоронних систем стає все вартіснішим й важчим. Таким чином, проведення дослідження щодо основних схем та засобів відмивання доходів, отриманих у сфері кіберзлочинності, на сьогодні є актуальним та необхідним.

Питання формування заходів попередження та профілактики кіберзлочинностів Україні в контексті забезпечення економічної безпеки та протидії правопорушенням у цій сфері ***є об'єктом дослідження*** багатьох науковців. Цій проблематиці присвячені праці, зокрема, Бутузова В., Карчерського М., Маркова В., Рудика М., Сезонова І., Скалозуба Л. та ін. Незважаючи на досить велику кількість публікацій, а також враховуючи останні зміни, що відбулися в законодавстві з даної проблематики, питання удосконалення сучасних напрямів протидії кіберзлочинам та відмиванню коштів, отриманих у сфері кіберзлочинності в Україні потребують додаткового розгляду.

Основною метою написання курсової роботи є формування ефективної системи заходів протидії та боротьби з кіберзлочинністю в Україні.

Для досягнення цієї мети запропоновано розглянути наступні **завдання:**

- дефініція суті кіберзлочинності та виявлення найбільш розповсюджених засобів вчинення кіберзлочинів;
- систематизація ознак та критеріїв для вчасного виявлення фінансових операцій, що можуть бути пов'язані з відмиванням доходів, отриманих у галузі кіберзлочинності;
- аналіз типових інструментів та методів відмивання доходів, отриманих у сфері кіберзлочинності;
- удосконалення сучасних напрямів протидії кіберзлочинам та відмиванню коштів, отриманих у сфері кіберзлочинності.

Об'єктом дослідження є феномен кіберзлочинності як загрози для економічної безпеки в інформаційній сфері.

Предметом дослідження є система запобігання і боротьби з кіберзлочинністю в Україні.

Вищевказані прерогативи даного виду злочину поряд з його значною прибутковістю стали безсумнівно істотними перевагами у порівнянні з іншими злочинами, скоєння яких в умовах покращання правоохоронних систем стає все вартіснішим й важчим. Таким чином, проведення дослідження щодо основних схем та засобів відмивання доходів, отриманих у сфері кіберзлочинності, на сьогодні є актуальним та необхідним.

1. КІБЕРЗЛОЧИННІСТЬ: ПОНЯТТЯ, ВИДИ, ЗАГРОЗИ ТА РИЗИКИ

Проблема пошуку шляхів протидії злочинам з уживанням інформаційно-комунікаційних систем уже доволі тривалий час знаходиться у центрі уваги як міжнародної спільноти, так й державних органів України зокрема. Беручи до уваги той факт, що піднесення технологій проходить швидше ніж приймаються нормативно-правові акти, котрими вони регулюються, а об'єми незаконно отриманих коштів кіберзлочинцями зростають, потрібно на сталій основі віднаходити шляхи вирішення нових проблем, пов'язаних з такими галузями, як транскордонний доступ правоохоронних служб до даних, захист даних та обмін інформацією між приватними та державними структурами. Міжнародна спільнота, зважаючи на імовірні негативні наслідки даного явища, знаходиться у стабільному пошуку заходів, котрі дозволяють зменшити загрози впливу кіберзлочинності на суспільство. Останніми роками спостерігається помітна активність в прийнятті регіональних та міжнародних документів, направлених на протидію кіберзлочинності, котрі включають як обов'язкові, так й необов'язкові до виконання правила. Відповідно до дослідження, здійснюваного 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 [2]:

- Ради Європи чи Європейського Союзу;
- Організації Об'єднаних Націй (далі – ООН);
- міжурядових африканських організацій;
- Ліги арабських держав;
- Співдружності незалежних держав або Шанхайської організації співробітництва.

Усі ці документи в повній мірі доповнюють один одного, у тому числі в частині, яка стосується підходів та концепцій, описаних в Конвенції Ради

Європи про злочинність у кіберпросторі, прийнятій 23 листопада 2001 року в Будапешті, Угорщина (далі – Будапештська конвенція). На сьогодні Будапештська конвенція є основою для розробки законодавства у сфері боротьби з кіберзлочинами як для загальносвітового законодавства, так і для кожної країни окремо. Будапештська Конвенція потребує від держав:

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

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

- розширювати міжнародне співробітництво з іншими країнами-учасницями Конвенції через загальні (взаємна допомога, екстрадиція, добровільне надання інформації) і спеціальні заходи (взаємна допомога щодо доступу до комп'ютерних даних, розкриття та термінове збереження збережених даних про рух інформації, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж). Комітет Конвенції проти кіберзлочинності («T-CY») був створений для того, щоб допомогти країнам-учасницям розглядати необхідність внесення доповнень або протоколів до Конвенції і обмінюватися інформацією. Крім того, в 2006 році Рада Європи ініціювала Міжнародний проект по боротьбі з кіберзлочинністю, котрий направлений на те, щоб сприяти країнам в питаннях навчання співробітників правоохоронних органів, вдосконалення законодавства, навчання органів прокуратури і суддівського корпусу, вироблення заходів для захисту персональних даних, зміцнення співпраці між державним і приватним

сектором,а також захисту дітей від насильства та сексуальної експлуатації. Власну стратегію щодо вирішення проблем протидії кіберзлочинності розроблено також Європейським поліцейським відомством («Європол»). На сьогодні «Європол» надає членам ЄС аналітичну і слідчу підтримку через свою базу даних злочинів і систему онлайн-розслідувань.

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

Помітну роль у подоланні проблем міжнародної співпраці у сфері боротьби з кіберзлочинністю відіграє ООН, котра приділяє велику увагу проблемам поширення злочинів, пов’язаних з використання комп’ютерних та інформаційних систем, та боротьби з таким злочинами. ООН неоднократно наголошувала на транснаціональному характері кіберзлочинів та потребі координації у світовому масштабі заходів щодо запобігання таким злочинам та їх розслідування.

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

З ціллю обмеження загроз та незахищеності в інформаційному просторі Міжнародним союзом електрозв’язку, як спеціалізованою інституцією ООН, розроблено: Вказівки для дітей щодо захисту в онлайновому середовищі; Вказівки для галузі щодо захисту дитини в онлайновому середовищі; Вказівки для батьків, опікунів та вчителів щодо захисту дитини в онлайновому середовищі; Вказівки для директивних органів щодо захисту дитини в онлайновому середовищі; Глобальну програму кібербезпеки.

Експертами Управлінням ООН з наркотиків і злочинності також зазначається, що форми міжнародного співробітництва включають надання взаємної правової допомоги, видачу злочинців, взаємне визнання іноземних судових рішень та неофіційне співробітництво між правоохоронними органами різних країн.

Крім того, змінний характер електронних доказів в рамках міжнародного співробітництва в кримінальних питаннях у галузі 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 заходів і стратегій, направлених на нейтралізацію потенційно шкідливих наслідків для суспільства і приватних осіб та зниження ризику скоєння злочинів.

До числа оптимальних заходів у напрямку попередження кіберзлочинності належать розвиток потенціалу органів кримінального правосуддя і правоохоронних органів, прийняття стратегій, законів щодо протидії кіберзлочинності, створення міцної бази знань і співробітництво між органами державного управління, ефективне керівництво, інформаційно-просвітницька діяльність, громадами, приватним сектором і на міжнародному рівні.

На сьогодні в українському законодавстві відсутнє визначення поняття «кіберзлочинність» або «кіберзлочин», є лише узагальнене поняття правопорушень і злочинів, що вчиняються з використанням комп'ютерних систем, комп'ютерів та мереж електрозв'язку (розділ XVI Кримінального кодексу України (далі – КК України)), зокрема [6]:

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 3611 КК України);
- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 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 3612 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);

- 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);

- перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 3631 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.

Експертами Управлінням ООН з злочинності і наркотиків також зазначається, що визначення поняття «кіберзлочинності» головним чином залежать від того, в яких цілях даний термін буде використовуватися. Засади кіберзлочинності становлять незначне число діянь, направлених проти цілісності, конфіденційності та доступності комп'ютерних систем або даних.

Проте, якщо цим не обмежуватися, то щодо вчинків, що передбачають уживання комп'ютера в цілях отримання фінансового або особистого прибутку або заподіяння фінансової або особистої шкоди, включаючи форми злочинів, пов'язаних з використанням персональних даних, і діяння, пов'язані з інформацією, яка зберігається в комп'ютері (усі вони входять в ширше поняття

«кіберзлочинність»), доволі проблематично знайти загальне юридичне визначення.

У глобальному плані спостерігається широкий діапазон кіберзлочинів, котрі включають злочини, пов'язані з використанням даних, які містяться в комп'ютері, злочини, що відбуваються в цілях отримання фінансової вигоди, а також злочини, спрямовані проти цілісності, конфіденційності та доступності комп'ютерних систем. Слід відзначити, що Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає умовну класифікацію кіберзлочинів, що поділяються на наступні категорії:

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

- втручання у систему, включаючи умисне створення серйозних перешкод функціонуванню комп'ютерної системи, приміром, шляхом розподілених атак на основну інформаційну інфраструктуру;
- нелегальне перехоплення комп'ютерних даних;
- втручання у дані, включаючи навмисне знищення, пошкодження, погіршення, приховування або зміну комп'ютерної інформації без права на це;
- незаконний доступ, наприклад, шляхом обману, злому і іншими засобами;
- зловживання пристроями, тобто виготовлення, придбання, продаж для розповсюдження, використання комп'ютерних програм, пристроїв, кодів доступу або комп'ютерних паролів з метою здійснення «CIA-злочинів»;

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

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

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

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

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

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

- приватної власності та господарських відносин, які включають в себе незаконні фінансові операції та заборонені види господарської діяльності, які здійснюються за допомогою комп'ютерних мереж чи мереж електрозв'язку.

Водночас, з урахуванням мотивації злочинців, кіберзлочини вбачається за можливе умовно поділити на наступні категорії [30; 31]:

- втручання в роботу інформаційних системи з ціллю отримання доступу до автоматизованих систем управління (для навмисного нанесення збитків конкурентам або для пошкодження за винагороду);

- кібершахрайство з ціллю заволодіння інформацією (для подальшого продажу або для власного користування);

- кібершахрайство з ціллю заволодіння коштами;

- інші злочини.

Перша категорія злочину – це присвоєння коштів, при якому шахраї використовують різні способи, іноді змушуючи користувачів самостійно розкривати конфіденційні дані. За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів [2]:

1) банкоматне шахрайство:

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

- використання «білого пластику» для зняття готівки в банкоматах та «клонування» або підробки платіжної картки;

- «Transaction Reversal Fraud» – втручання в роботу банкомату при виконанні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при реальному отриманні готівки зловмисником;

- «Cash Trapping» – заклеювання диспенсеру для привласнення зловмисником готівки, котра була списана з карткового рахунку законного держателя картки;

2) шахрайство в торгівельно-сервісних мережах:

- операції без проведення авторизації на суму нижче встановленого ліміту;

- викрадення реквізитів платіжних карток, у тому числі із вживанням технічних засобів та їх «клонування»;

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

- використання втрачених, викрадених або підроблених платіжних карток;

3) шахрайство в Інтернет мережі:

- викрадення реквізитів платіжних карток;

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

- проведення операцій із вживанням викрадених реквізитів платіжних карток.

4) шахрайство в системах дистанційного банківського обслуговування:

- проведення несанкціонованих операцій, відкриття рахунків та отримання готівки в результаті несанкціонованих операцій у системах дистанційного банківського обслуговування;

- створення троянських програм та комп'ютерних вірусів для прихованого перехоплення управління комп'ютером клієнта з встановленим програмним забезпеченням дистанційного банківського обслуговування;

- отримання платежів через міжнародну систему SWIFT від закордонних відправників внаслідок втручання у роботу комп'ютерів та систем дистанційного банківського обслуговування клієнтів закордонних банківських установ.

Найпоширеніші злочини, котрі відносяться до третьої та другої категорії – це виведення з ладу комп'ютерних систем компаній і урядових організацій та злом баз даних. Також широко розповсюдженими є крадежі технологій або інновацій і, звичайно, банальна крадіжка грошей.

Одна із найбільш поширених схем, коли шахраї крадуть дані зарплатних рахунків співробітників компаній, котрі в подальшому продають їх на чорному ринку. Розцінки на таку специфічну інформацію розпочинаються від кількох доларів США за рахунок. Є й інший варіант – залишити ці дані собі й просто перевести гроші на свій рахунок з сотень і тисяч банківських карт.

У межах даної курсової роботи розглядаються кіберзлочини, що здійснюються з ціллю або внаслідок яких виникає фінансова або інша матеріальна вигода у формі незаконно отриманих доходів. В першу чергу, мова йде про використання комунікаційно-інформаційних систем та комп'ютерних технологій для доступу до приватної власності фізичних та юридичних осіб та подальших дій щодо розпорядження чи управління цією власністю. Зокрема, найбільшого розповсюдження зараз серед кіберзлочинів набрало отримання доступу до коштів клієнтів банківських установ.

Варто зазначити, що швидкий розвиток сфери інформаційних технологій безперервно генерує модерні види послуг, в тому числі у фінансовій сфері. Це, в свою чергу, змушує зловмисників вдосконалювати власні здібності та вигадувати нові способи незаконного заробітку в кібер-середовищі.

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 класифікацій 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 [10, с.10].

Таблиця 1

Об'єкти виникнення загроз та кількість атак

на світовому ринку кіберзлочинності у 2011-2013 р.р. [32]

Об'єкт	2011 р. (к-ть атак)	2013 р. (к-ть атак)	Відхилення (%)
E-mail	2414	2622	8,6
Нове покоління брандмауерів	2249	3217	43,0
Система захисту від вторгнень	1890	1906	0,8
VPN	941	746	-20,7
Споживачі	4451	4916	10,4
Криміналістика	221	369	67,0
Політика	801	962	20,1
Безпека систем управління	201	166	-17,4
Консалтингові послуги	4366	4694	7,5

Джерело: Складено автором за даними: Net Losses Estimating the Global Cost of Cybercrime [Electronic Source] / Center for Strategic and International Studies. – 2014/ - Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Як видно з табл..1., найбільша кількість кібератак прийшлася у 2014 році на введення в оману споживачів, а також на надання консалтингових послуг. Хоча найбільше відхилення у 2013 р. в порівнянні до 2011 року спостерігаємо за сферою криміналістичної діяльності. Позитивна тенденція спостерігається відносно VPN та безпеки систем управління.

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.

Розглянемо рівень кіберзлочинності у 2014 році у розрізі країн світу:

Таблиця 2

Рівень кіберзлочинності країн світу у 2014 р. (% від ВВП) [32]

Країна	Показник (% від ВВП)	Приналежність до G20
Канада	0,17	X
Італія	0,04	
Китай	0,63	X
Нідерланди	1,50	
Росія	0,10	X
Німеччина	1,60	X
Сінгапур	0,41	
Великобританія	0,16	X
США	0,64	X
Австралія	0,08	

Джерело: Складено автором за даними: Net Losses Estimating the Global Cost of Cybercrime [Electronic Source] / Center for Strategic and International Studies. – 2014/ - Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Як видно з табл..2, найвищий показник кібератак припав на Німеччину та Нідерланди, а найменший – на Австралію та Італію. Водночас, варто зазначити,

що вищим рівнем показника за кількістю кібератак у 2014 році характеризувалися країни G20, а значно нижчим менш розвинуті країни.

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.

Проблеми кібербезпеки вимагають нових критичних підходів до розуміння технологічних і соціальних ризиків, що виникають у цій сфері, а відтак, майбутні політичні завдання можуть бути вирішені тільки тоді, коли буде визначено характер проблеми належним чином. У даній курсовій роботі розглянуто літературу у сфері боротьби з кіберзлочинністю, відповідаючи на питання дослідження і його здатності генерувати уявлення про структуру управління тією чи іншою галуззю безпеки. Кібербезпека є областю, яка до сих пір недостатньо вивчена. В результаті, важливо зосередитися на концепціях, які мають значення для обговорення співпраці, безпеки та управління.

Кібербезпека вважається політичною, економічною і соціальною загрозою, яка постійно розвивається в усьому світі. Те, як розуміється безпека, котра швидко розвивалася протягом останнього сторіччя, що вплинуло на парадигми безпеки, ґрунтується на оцінці ризику. У даній роботі, основна увага приділяється Європі та Україні зокрема, що визначається її географічним, культурним або історичним критеріям. Сучасне розуміння європейської безпеки є прямим наслідком воєн і конфліктів в минулому столітті. Протягом багатьох років територіальні війни і конфлікти змінили ландшафт безпеки за межами військового підходу, і безпека прогресувала від того, щоб бути чистим захисним механізмом, до більш широкого поняття, в тому числі невійськової безпеки. Однак загроза не є статичною концепцією , а визначення не може бути прикріплене до однієї з цих цілей. Замість цього важливо, щоб зв'язати

розуміння як загрози і безпеки для конкретного місця і часу, так як ці два поняття розрізняються між окремими людьми, ситуаціями, умовами і часом.

Створення інституцій в ЄС, наприклад, «Європол» і «Судове співробітництво Європейського Союзу (Євроюст)» підвищує рівень гармонізації права і, таким чином, дає менше можливостей для транснаціональних кібертерористів використовувати регіональні прогалини в нормативно-правовому регулюванні. Існують країни, які не визнають цю проблему, або вони мають різне тлумачення кіберризиків. Це створює значні перешкоди для подальшого розвитку випереджаючих форм управління. Ці проблеми не тільки пов'язані з міжнародним співробітництвом на стратегічному рівні; одні й ті ж бар'єри видно на оперативному рівні. Наприклад, Росія відмовилася співпрацювати в випадку з Естонією (2007 р.) в питаннях розслідування кібератак. Те ж саме відбулося в Литві (2008 р.), Грузії(2008 р.), Україні (2013-2016 р.р.). Прикладом є також ситуація з Китаєм, який заперечує всі причетності до кібератак. І Росія, і Китай блокують міжнародне співробітництво і розвиток договорів, і це створює значний регрес для розробки заходів протидії кібертероризму.

2. КРИМІНАЛЬНОЛОГІЧНИЙ АНАЛІЗ ДОХОДІВ У СФЕРІ КІБЕРЗЛОЧИННОСТІ ТА ОСОБЛИВОСТЕЙ ЇХ ЛЕГАЛІЗАЦІЇ

В новітніх умовах системи дистанційного банківського обслуговування («Інтернет-Клієнт-Банк», «Клієнт-Банк», «Інтернет-банкінг») стали невід'ємною частиною фінансової системи як в Україні, так і у всьому світі. Система дистанційного банківського обслуговування – це багатофункціональний програмно-технічний комплекс, що дає можливість клієнтам банку контролювати стан своїх рахунків, опрацьовувати і скеровувати в банк на виконання платіжні та інші документи, а також одержувати широкий спектр актуальної фінансової інформації без прямого звернення до банку. Дистанційне банківське обслуговування – загальна категорія для технологій надання банківських послуг на підставі розпоряджень, переданих клієнтом віддалено (тобто, без візиту до банку). Вживання системи дистанційного банківського обслуговування безсумнівно має свої переваги. Передусім варто виділити наступні:

- зручність і простота. Автоматизація процесу підготовки платіжних та інших документів, а також наявність програмного ревізування щодо заповнення обов'язкових реквізитів у документах суттєво спрощує користування підсистемами і дає можливість мінімізувати операційні помилки;
- економічність та оперативність. Вживання системи дистанційного банківського обслуговування дає можливість з офісу реалізувати управління фінансовими потоками підприємства й суттєво скорочує витрати робочого часу персоналу, пов'язані з відвідуванням банку;
- ефективність та безпека. Система дистанційного банківського обслуговування, за умови правильного використання, дає можливість збільшити конфіденційність і безпеку документообігу з банком; в будь-який момент одержати виписку, що включає інформацію про всі вихідні і вхідні документи в розширеному форматі, без відвідування банку.

В той же час, системи дистанційного банківського обслуговування, як інструмент доступу до грошових переказів, зараз все частіше стають ціллю для кіберзлочинців. Втручання в діяльність систем дистанційного банківського обслуговування найчастіше проходить шляхом зараження комп'ютера вірусним програмним забезпеченням через відвідування заражених сайтів, шкідливу спам-розсилку або вживання заражених магнітних носіїв. Завантаження вірусу на комп'ютер відбувається фактично непомітно. Фундаментальне завдання вірусу на початковому етапі – це збір інформації, спостереження і передача на комп'ютер шахраїв. Вірус потенційно може викрадати ключі електронного цифрового підпису, паролі доступу до систем дистанційного банківського обслуговування, зчитувати реквізити платежів. Це також можуть бути програми, які відстежують появу на екрані вікна підключення до дистанційного банківського обслуговування з ціллю наступного перехоплення секретної інформації, котра вводиться в це вікно, або копіюють вміст буфера обміну в момент підключення до систем електронних платежів.

Ціль шахраїв - спотворити інформацію, сформувати за допомогою дистанційного банківського обслуговування і виконати платіж, котрий за змістом не буде визначатися в потоці звичайної діяльності жертви, але переведе гроші на рахунки фіктивної фірми або підставної особи, використовуючи звичайне для даного клієнта призначення платежу. В подальшому найчастіше кошти вкрадені з рахунку переводяться в готівку. Зняття готівки відбувається в основному через банкомати з ціллю уникнення спілкування з працівниками банку.

Платіжні картки в теперішніх умовах є не лише способом нарахування пенсії, отримання заробітної плати, або інших зарахувань, але й зручним та ефективним інструментом для повноцінного банківського обслуговування. Вживання платіжних карток дає змогу:

- здійснювати операції не лише в національній валюті, але в іноземній (використовуються мультивалютні картки);

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

- проводити розрахунки в різних країнах світу цілодобово.

Ринок платіжних карток зростає в Україні досить стрімкими темпами (більше 25% на рік). Так, за інформацією Національного банку України станом на 1 жовтня 2015 року в Україні перебуває в обігу 78,1 млн. платіжних карток, з яких 43,9 млн. карток були активними. При цьому, сума операцій, проведених з використанням платіжних карток, за 9 місяців 2015 року склала близько 750,0 млрд. грн..[9]. Помітні обсяги фінансових операцій з вживанням платіжних карток є основним фактором, який привертає до цієї галузі особливу увагу злочинців. З ціллю заволодіння коштами держателів платіжних карток злочинці вигадують найрізноманітніші прийоми. Це, наприклад, можуть бути:

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

- електронні пристрої, котрі дозволяють зчитувати потрібну інформацію з клавіатури банкомату або з платіжної картки;

- підробка платіжних карток з використання викраденої інформації;

- технічні пристрої, котрі встановлюються на банкомат з ціллю заволодіння грошима або платіжною карткою;

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

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

- написання імені та прізвища клієнта латиною;

- номер картки;

- дата випуску або завершення дії картки;

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

- секретне питання (прізвище матері, найкращого друга тощо);

- ПІН-код.

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

В межах даної курсової роботи ми під кібершахрайством розуміємо шахрайство, здійснене з використанням комп'ютерних мереж, комп'ютерів, в тому числі з використанням Інтернет мережі.

Варто зазначити, що в сьогоднішніх умовах у віртуальне середовище переходить помітна частина традиційного бізнесу, що пояснюється стрімким розвитком Інтернет мережі. Це передусім стосується розміщення в Інтернет мережі реклами послуг і товарів, а також Інтернет-торгівлі, котра є достатньо розповсюдженою в Україні та, у певних сферах, складає значну конкуренцію традиційній торгівлі.

Шахраї так само застосовують новітні можливості Інтернет мережі для своїх оборудок. Доволі розповсюдженими є:

- створення «фінансових пірамід» в мережі Інтернет (наприклад, «Helix»);

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

- розміщення шахрайських оголошень щодо збору коштів (наприклад, благодійні пожертви) та ін.

В межах даної курсової роботи, до кіберзлочинів нефінансового характеру, віднесемо злочини у кіберпросторі, що безпосередньо не стосуються переказу коштів та сфери фінансових послуг. Проте, одержання незаконних доходів є фундаментальною метою скоєння і цих злочинів.

До таких злочинів, на думку автора, варто віднести [1, с.17]:

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

- залякування, кібер-здирництво, поширення неправдивої інформації та наклеп в Інтернет мережі;

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

- проведення заборонених азартних ігор онлайн;

- викрадення особистої або ділової інформації;

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

На відміну від «традиційного» відмивання фінансів, для реалізації якого використовується банківська система, кібер-відмивання базується на вживанні різних видів постачальників фінансових послуг і операцій, починаючи з банківських переказів, внесення та зняття готівки, застосування електронних грошей, і закінчуючи послугами з переказу грошей. Зазвичай ланцюжок переривається на операції з готівковими засобами, здійснювану зазвичай «грошовими мулами», за якою іде вживання традиційної платіжної системи.

Якщо придатний платіжний сервіс інтегрований з послугами з онлайнових платежів, то кошти можуть бути переведені на електронні і без очікування практично анонімно переведені в іншу країну. Таким чином, виявлення і переслідування кримінальних грошових потоків є дуже тонким завданням для правоохоронних органів. Такі складні схеми є викликом сильному, але традиційному програмному забезпеченню для збору даних у галузі протидії відмиванню доходів та фінансуванню тероризму, заснованому на поведінці споживачів, якщо частина «відмивального» ланцюжка здійсняється абсолютно в іншій фінансовій ситуації.

Методи здійснювання платежів в системі Інтернет, можуть також розділяти джерело, звідки прийшли інструкції на здійснення операції від реального місця реалізації грошового переказу. Це є ще однією перешкодою для

правоохоронних органів в частині виявлення і переслідування злочинних доходів.

Отримані злочинним шляхом доходи вимагають від злочинців ефективного та швидкого проведення їх легалізації. При чому, з огляду на особливості кіберзлочинності – виконавці та організатори схем переважно є технічно грамотними та освіченими, відповідно і методи, які ними використовуються при легалізації отриманих коштів, можуть теж бути суттєво нестандартними та складними. Механізми та інструменти, якими користуються злочинці під час виконання процесу відмивання доходів, одержаних у галузі кіберзлочинності, є дуже різноманітними, наприклад, при відмиванні доходів від кіберзлочинів характерним є використання наступних механізмів:

- проведення ланцюга фінансових операцій через декілька банківських рахунків за допомогою віддаленого доступу;
- вживання альтернативних платіжних систем (наприклад, електронні платежі), як національних, так й міжнародних;
- купівля електронних грошей та вживання систем платежів через електронні гаманці;
- застосування рахунків, відкритих особами на підставних осіб, за втраченими документами;
- використання готівки на останньому етапі ланцюга фінансових операцій;
- конвертація незаконних доходів у товари шляхом надбання останніх через Інтернет мережу.

Переведення викрадених коштів у готівку є розповсюдженим, оскільки наступне переміщення готівки поза межами банківської системи практично неможливо відслідкувати. Докладно практикується зняття готівки через банкомати з ціллю уникнення комунікації учасників схеми з працівниками банківських інституцій. В подальшому готівкові кошти через кур’єрів (так званих «грошових мулів») можуть бути вільно передані анонімному організатору кіберзлочину. Одержані кримінальним шляхом кошти

використовуються для купівлі високоліквідних товарів або передплачених карток для наступного їх перепродажу і одержання готівки.

Також кошти можуть бути використані для купівлі через Інтернет проїзних документів, квитків, предметів побуту та інших товарів для наступного їх використання, отримання та перепродажу готівкових грошових коштів. Частка кримінальних доходів використовується на придбання нового обладнання та розробку більш продуктивного шкідливого програмного забезпечення з тим, щоб оминути системи безпеки. Варто зазначити також, що основами для платежів, пов'язаних з несанкціонованим списанням коштів, можуть бути різні призначення, котрі не дають перспективи відокремлювати їх від інших фінансових операцій:

- оплата послуг (роботи по контролю якості продукції, перевезення вантажу, рекламно-поліграфічні послуги, транспортно-експедиційне обслуговування, проведення спортивних змагань);
- оплата за господарчі товари, металовироби, прилади, обладнання, нафтопродукти, будматеріали, офісні меблі, соняшник, олія соняшникова);
- оплата по договору;
- надання та повернення фінансової допомоги (так званої позики);
- сплата відрядних або заробітної плати;
- поповнення карткового рахунку;
- сплата за рішенням суду;
- повернення гарантійного внеску учаснику торгів за договором.

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

З ціллю швидкого та зручного переказу коштів, одержаних у галузі кіберзлочинності, злочинцями широко використовуються резерви систем переказу коштів або платіжних систем. Законодавство України передбачає діяльність в Україні міжнародних та внутрішньодержавних платіжних систем. Внутрішньодержавна платіжна система – платіжна система, в якій платіжна

організація є резидентом, та яка реалізовує 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 котра 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 01.07.2015 р. на території України здійснювали діяльність з переказу коштів дев'ять міжнародних і внутрішньодержавних систем переказу коштів, створених резидентами України, із котрих п'ять систем запроваджені банками та чотири системи – небанківськими інституціями України. Теж на території України функціонують 22 міжнародні системи переказу коштів, створені нерезидентами. Учасниками таких систем є більше 150 банків України, національний оператор поштового зв'язку УДППЗ «Укрпошта»ПрАТ та «Українська фінансова група». У І півріччі 2015 року з використанням міжнародних та внутрішньодержавних систем переказу коштів, створених як резидентами, так і нерезидентами, було переказано:

- у межах України – 7 915,0 млн. грн. та 4,5 млн. дол. США (в еквіваленті);
- в Україну – 2 203,0 млн. дол. США (в еквіваленті);
- за межі України – 384,0 млн. дол. США (в еквіваленті)[9].

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

- мобільність – користувач через мережу Інтернет може виконувати управління своїм рахунком з будь-якого місця;
- оперативність – транзакції по рахунку проходять протягом декількох секунд;
- простота використання – використання та відкриття електронного рахунку є інтуїтивно прозорим і не потребує спеціальних знань;
- доступність – відкриття власного електронного рахунку є безкоштовним для будь-якого користувача;

- безпека – передача інформації ведеться з вживанням криптографічного захисту.

Щоб стати учасником і уживати послуги платіжної системи необхідно пройти процес реєстрації й відкрити в ній електронний рахунок у вигляді електронного гаманця. Електронний гаманець пам'ятає інформацію про суму коштів на рахунку користувача в платіжній системі.

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

Крім того, для переміщення готівкових коштів між учасниками схеми можуть застосовуватися термінові перекази через міжнародні системи переказу коштів. Механізм такого роду переказів є досить зручним та простим. Для цього у відділення системи або її партнера звертається особа (потрібно мати документ, котрий засвідчує особу), що вносить потрібні кошти та заповнює бланк із зазначенням ім’я і прізвища отримувача та країни відправлення переказу. В наступному від оператора отримується номер переказу, який потрібно 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, країни відправлення переказу, ім’я та прізвища відправника, валюти та суми переказу. Здійснення переказу та отримання готівки займає тільки кілька хвилин.

Використання електронних грошей для відмивання доходів. За законодавством України електронні гроші – це одиниці вартості, котрі приймаються як засіб платежу іншими, ніж емітент, особами, зберігаються на електронному пристрої, і є грошовим зобов’язанням емітента. Випуск електронних грошей в Україні мають право реалізувати лише банки (емітенти). Останні мають право виконувати випуск електронних грошей, виражених лише в гривнях. Сума електронних грошей на електронному пристрої, котрий не

може поповнюватися, не повинна перевищувати 2 тис. грн. Сума електронних грошей на електронному пристрої, котрий може поповнюватися, не повинна перевищувати 8 тис. грн. [27]

Погашення електронних грошей, пред'явлених користувачами – фізичними особами, може здійснюватись готівковими коштами чи шляхом переказу на банківський рахунок пред'явника. Погашення електронних грошей, пред'явлених користувачами – суб'єктами господарювання, агентами, торговцями, емітент зобов'язаний реалізовувати виключно шляхом переказу на їх банківські рахунки. За допомогою електронних грошей припустимо здійснювати наступні платежі:

- купівля ж/д та авіаквитків, бронювання готелів;
- оплата комунальних та Інтернет-послуг;
- оплата товарів в Інтернет-магазинах;
- платежі всередині системи на рахунки юридичних та фізичних осіб;
- оплата послуг операторів мобільного зв'язку;
- купівля палива та замовлення паливних скретч-карт;
- оплата мита, державних зборів та штрафів;

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

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

Суттєво швидкий розвиток комп'ютерних та інформаційних технологій останнім часом призводить до швидкого розвитку кіберзлочинності, тому характерної актуальності зараз набувають питання попередження і протидії злочинствам у кіберпросторі. Попередження кіберзлочинності ґрунтується на заходах спрямованих на зниження ризику реалізації подібних злочинів та нейтралізацію шкідливих ефектів для приватного сектору та суспільства. Дійова протидія кіберзлочинам повинна пов'язувати комплекс законодавчих, організаційних, технічних та інформаційних заходів.

На законодавчому рівні в Україні лишається невирішеними багато питань у галузі протидії кіберзлочинності. Це передусім, відсутність у вітчизняному законодавстві твердого визначення категорії «кіберзлочинність». Дефініція такої категорії може дати помітний поштовх до приведення у відповідність інших нормативно-правових актів. Удосконалення законодавчого забезпечення у галузі протидії та попередження легалізації прибутків, пов'язаних із злочинами у галузі кіберзлочинності, імовірне за такими напрямами:

- внесення змін до Кримінального кодексу України в частині посилення відповідальності за злочини у галузі інформаційних та комп'ютерних технологій;
- визнання електронних документів та новітніх даних у якості доказової бази в процесі розслідуванні кіберзлочинів;
- чітка регламентація механізмів взаємозв'язку між банком та клієнтом, між підприємством та його контрагентом;
- закріплення вимоги щодо неухильного проведення обов'язкового online-інформування клієнтів про кожну здійснену операцію та двоканальної аутентифікації;

- впровадження практики ідентифікації користувача Інтернет шляхом надання ідентифікаційного коду індивіда оператору зв'язку, при подачі письмової заяви про укладення контракту на надання послуг;

- зобов'язання банків безоплатно в обов'язковому порядку підключати послугу СМС повідомлення у контексті здійснення будь-яких операцій за поточними картковими рахунками;

- впровадження сертифікації електронних платіжних засобів;

- зобов'язання банків установити антискімингові прилади на всіх банкоматах;

- зобов'язання банків щодо перспективи проведення вихідних платежів клієнтів лише за рахунок остатків на їх рахунках на початок операційного дня. У подібному випадку, банк, в якому відбулось несанкціоноване списання коштів, та клієнт, який поніс втрати, будуть мати додатковий час для можливості блокування коштів на рахунку недобросовісного отримувача;

- встановлення фіксованого граничного розміру видачі готівки, яка може проводитись в позаопераційний час банку по одному картковому рахунку через банкомат і котрий неможливо змінювати;

- запровадити реєстрацію в податкових органах Інтернет-магазинів стосовно конкретних платників податків.

З ціллю попередження кіберзлочинів банківськими установами можуть упроваджуватись наступні організаційні та технічні заходи:

- систематичний огляд банкоматів для виявлення незаконно встановлених приладів;

- обов'язкове повідомлення клієнтів про кожну здійснену операцію;

- введення «чорного» реєстру рахунків (ЄДРПОУ, ДРФО, кодів IP- адрес) шахраїв для вчасного блокування операцій;

- запровадження для клієнтів банку карток з мікропроцесором (чіпом), як більш захищених від фальсифікації;

- правила щодо двоканальної (двофакторної) аутентифікації;

- вживання токенів для зберігання цифрових електронних підписів користувачів;

- вживання ряду логічних правил для підозрілих платежів в системі Інтернет-банкінгу;

- підтвердження здійснених проплат в телефонному режимі;

- статистичний аналіз трафіку Netflow для виявлення відхилень;

- вживання клієнтом самостійного комп'ютеру, котрий призначений тільки для системи Інтернет-банкінг, з налаштованими міжмережевими фільтрами;

- генерація клієнтського ключа власне клієнтом, що унеможливлює здійснення неправомірних правочинів збоку працівників банку;

- встановлення обмежень на здійснення операцій у певних ризикових країнах;

- взаємоприв'язка ключа клієнта та серійного номеру жорсткого диску/ дискети / флеш накопичувача, що унеможливлює копіювання ключів системи Інтернет-банкінгу та доступ до сторінки клієнта за умовою використання інших комп'ютерів;

- встановлення обмежень на здійснення операцій у системі Інтернет;

- встановлення обмежень на здійснення операцій за їх періодичністю.

Варто зазначити, що помітна частина кіберзлочинів, стає здійснимою завдяки некомпетентності населення те порушенню основних правил безпеки.

Такими факторами зокрема є:

- незначна кількість інформації та даних про кіберзлочини;

- низький рівень обізнаності про ризики, спричинені запровадженням нових платіжних сервісів та систем, а також щодо пов'язаного з ними відмивання грошових коштів;

- нехтування елементарними нормами безпеки при користуванні Клієнт-банком та спеціальними платіжними засобами в мережі Інтернет;

- сумнівне зберігання цифрового електронного підпису та паролів клієнтами банківських установ;

- використання та встановлення неліцензійного програмного забезпечення (наприклад, антивіруси, операційні системи);

- невиконання політики парольної та інформаційної безпеки.

У зв'язку з цим, помітну користь у попередженні кіберзлочинності, мають просвітницько-інформаційнї заходи щодо модерних ризиків та загроз в комп'ютерних та інформаційних системах. Національним банком України з ціллю 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».

Незважаючи на досвідченість кіберзлочинців та вживання ними широкого інструментарію схем для легалізації незаконних доходів, являється потенційно можливим виокремити фінансові операцій за ступенем ризику. Більше того, ймовірно також схарактеризувати послуги та сфери, котрі мають підвищений ризик та відповідно вимагають підвищеної уваги. Індикаторами підозрілості фінансових операцій зазначеної скерованості для банківських установ опосередковано можуть бути наступні чинники:

- спроба вживання прострочених первинних робочих або старих ключів після сертифікації нових;

- трансакції в нестандартний час чи підключення у вечірній час до системи;

- спроба входу із нового чи забороненого IP–адресу;

- вживання для банківських операцій імен та IP-адресів користувачів, за якими попередній моніторинг розкрив відношення до шахрайських операцій;

- особливі умови або складність діяльності: висока частота переказувань коштів протягом незначного періоду часу, значна кількість різних основ походження коштів та платіжних інструментів;

- суб'єкт не інформована про природу функціонування юридичної особи, яку вона репрезентує;

- спроби в день зарахування зняти кошти;

- здійснення операцій за втраченими документами;

- суб'єкт не може пояснити закономірність надання тієї або іншої банківської послуги;

- притягнення до проведення дій осіб молодого віку або новостворених підприємств;

- дані операції не відповідають попереднім операціям клієнта;

- відкриття рахунку, на котрий зараховуються кошти врезультаті несанкціонованого списання, незадовго до здійснення такого роду операцій;

- намагання клієнта одержати дві або більше банківських карток, що не відповідає змісту його діяльності;

- зарахування коштів на карткові рахунки фізичних осіб із наступним зняттям через банкомати;

- відсутність даних щодо господарської діяльності суб’єкта господарювання або використання замість традиційних он-лайн платіжних систем;

- міжнародні перекази, які перераховуються за межі країни або надходять в країну, що не відповідає діяльності суб’єкта господарювання.

ВИСНОВКИ

Незважаючи на брак на сьогодні загальноприйнятної дефініції поняття «кіберзлочин» спостерігається доволі вичерпне та широке розуміння його змісту та способів реалізації, а також ризиків та загроз, що дає можливість формувати та запроваджувати заходи протидії даному виду злочину та боротьби з ним. Відсутність прямого зв'язку з представниками фінансової інституції, а також швидкість, анонімність реалізації та невисока вартість злочину стали фундаментальними передумовами зростання зацікавленості злочинців власне кіберпростором.

Інтернет-простір став не лише місцем здійснення злочину та отримання незаконного прибутку, а й місцем легалізації такого роду доходу. При цьому різноманіття видів кіберзлочинів у сукупності з різноманітністю методів та способів відмивання доходів, отриманих від реалізації даних видів злочинів, призводять до утруднення їх виявлення та розслідування. Виявлені схеми та механізми відмивання доходів, отриманих від кіберзлочинності, дають перспективи стверджувати, що переміщення коштів потенційно можливе як традиційними шляхами переказу, так і з застосуванням новітніх систем електронних грошей, термінових переказів та електронних платіжних систем. При цьому, кошти використовуються в одних випадках для придбання товарів або послуг в мережі Інтернет, передплачених карток, а в інших переводяться у ігрові фішки казино або електронні гроші та перераховуються між електронними гаманцями, з наступним переведенням у готівку.

У свою чергу, застосування готівки залишається одним з найбільш поширених методів та способів приховування як подальшого руху незаконного доходу та шляхів його вкладення, так й джерел походження таких коштів під час введення коштів до банківської системи. Це дає можливість злочинцям підтримувати подальшу анонімність, отриману на етапі отримання незаконного доходу, й під час відмивання доходів.

Протидія кіберзлочинам та боротьба з даним явищем поєднує комплекс технічних, правових, інформаційних та організаційних заходів, при цьому роль кожного з цих заходів не може бути охарактеризована другорядною чи пріоритетною. При цьому ефективна протидія відмиванню злочинних доходів та зниження рівня злочинності в цій галузі можливі завдяки своєчасному прояву фінансових операцій, що можуть бути пов’язані з відмивання доходів, отриманих у галузі кіберзлочинності, та ефективному співробітництву між приватним та державним сектором.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «кіберзлочинність» / В. М. Бутузов // Інформаційна безпека людини, суспільства, держави. – 2014. – № 1(3). – С. 16-18.
2. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку / М. В. Карчевський // Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення : матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 61-64.
3. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : [моногр.] / Карчевський М. В. – Луганськ : Луган. держ. ун-т внутр. справ, 2012. – 327 с.
4. Карчевський М. В. Основні напрями вдосконалення кримінально- правового забезпечення інформаційної безпеки / М. В. Карчевський // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 54-58.
5. Кіберзлочинність та відмивання коштів [Електронний ресурс] / Департамент фінансових розслідувань. Державна служба фінансового моніторингу. – 2013. – Режим доступу:
http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf
6. Кримінальний кодекс України [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу: http:// zakon1.rada.gov.ua
7. Литвинов М. Деятельность управления по борьбе с киберпреступностью МВД Украины на современном этапе [Электронный ресурс]. – Режим доступу : http: //cybersafetyunit.com/deyatelnost-upravleniya-po-borbe-s-kiberstupnostyumvd-na-sovrtmennom-etape/.– 01.07.2015/

8. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації / В. В. Марков // Південноукраїнський правничий часопис. – 2013. – № 1. – С. 112-115.

9. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект / В. В. Марков // Право і безпека. – 2015. – № 2. – С. 136-140.

10. Марков В. В. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види / В. В. Марков // Вісн. Харк. Ун ту внутр. справ. – 2014. – № 2. – С. 139-147.

11. Меживой В. П. Способи оперативного виявлення несакціонованого втручання в роботу автоматизованих систем та комп'ютерних мереж / В. П. Меживой // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали всеукр. наук. – практ. конф., 4 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 115-119.

12. Погорецький М. Кіберзлочини : до визначення поняття / М. Погорецький, В. Шеломенцев // Вісн. прокуратури. – 2012. – № 8. – С. 89-96.

13. Поляруш О. О. Використання мережі Інтернет як каналу інформаційно-психологічного впливу / О. О. Поляруш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2015. – № 21. – С. 218-227.

14. Ращенко Є. Кримінально-правове забезпечення боротьби зі злочинами у сфері використання комп'ютерних технологій / Є. Ращенко // Право України. – 2013. − № 10. – С. 87-91.

15. Розенфельд Н. Віртуальний предмет злочинів, пов'язаних з порушенням авторського права і суміжних прав / Н. Розенфельд // Право України. – 2012. − № 5. – С. 105-109.

16. Рудик М. В. Суб'єкт злочину, передбаченого ст. 362 КК України / М. В. Рудик // Роль та місце ОВС у розбудові демократичної правової держави. – Одеса, 2012. – С. 323-324.

17. Сабадаш В. П. Интернет-мошенничество: понятие, структура и динамика развития / В. П. Сабадаш // Актуальные проблемы современной криминалистики. – Минск , 2010. – С. 136-143.

18. Сапальов В. П. Особливості огляду місця події при розслідуванні злочинів в комп'ютерній сфері / В. П. Сапальов // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали всеукр. наук. – практ. конф., 4 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 179-182.

19. Сезонова І. К. Попередження неправомірних діянь при використанні інформаційних систем / І. К. Сезонова, Т. П. Колісник // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук. практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 68-76.

20. Семенов Г. Криминалистическая классификация преступлений против информации в системе сотовой связи / Г. Семенов, Н. Карпов // Закон и жизнь. – 2015. − № 5. – С. 24-28.

21. Семенов Г. Система сотовой связи как основополагающий фактор, детерминирующий способы совршения мошеничества в системе сотовой святи // Г. Семенов, Н. Карпов // Закон и жизнь. – 2014. − № 3. – С. 20-24.

22. Сервецький І. В. Деякі проблеми захисту персональних даних в Україні / І. В. Сервецький, В. В. Редька // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2014. – № 9. – С. 193-199.

23. Симкин Л. Как бороться с «сетевыми пиратами» / Л. Симкин // Рос. юстиция. – 2012. – № 7. – С. 62-64.

24. Скалозуб Л. П. Інтелектуалізація злочинності. Варіант стримування / Л. П. Скалозуб, В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2012. – № 1. – С. 295-307.

25. Скалозуб Л. П. Стан захисту інтелектуальної власності та протидії комп'ютерній злочинності: проблемні питання вирішення / Л. П. Скалозуб // Організація протидії у сфері інтелектуальної власності та комп'ютерних технологій : доповіді провідних вчених, представників громадськості,

державних службовців та працівників підрозділів ДСБЕЗ на міжвід. сем. – К., 2014. – С. 5-12.

26. Солодка О. М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України / О. М. Солодка // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., 17 берез. 2010 р., м. Київ. – К. : Нац. акад. СБУ України, 2010. – С. 126-128.

27. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення /А. В. Ставер // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 144-147.

28. Струков В. М. Деякі технічні аспекти побудови кіберпростору в контексті протидії кіберзлочинності / В. М. Струков // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 65-68.

29. Струков В. М. Технічні аспекти побудови кіберпростору, що сприяють кіберзлочинності / В. М. Струков // Боротьба з інтернет-злочинністю : матеріалиміжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид.ін-т, 2013. – С. 234-235.

30. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Економічні науки. - К. : УДУФМТ, 2014. - № 5-6 (76-77). - С. 125-130.

31. Якубівська Ю. Є. Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі / Ю. Є. Якубівська // Вітчизняна система охорони і захисту інтелектуальної власності в умовах приєднання до Європейського Союзу: Збірник тез доповідей Всеукраїнської науково-практичної конференції, м. Тернопіль, 24-25 квітня 2015 р., ТНЕУ. – Тернопіль, 2015. – С. 164-166.

32. Net Losses Estimating the Global Cost of Cybercrime [Electronic Source] / Center for Strategic and International Studies. – 2014/ - Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf