МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Юридичний факультет
Кафедра безпеки, правоохоронної діяльності та фінансових розслідувань

ЯКОБЧУК Анастасія Андріївна

Протидія кіберзлочинності в банківській сфері / Combating cybercrime in the banking sector

спеціальність: 073 - Менеджмент
освітньо-професійна програма - Управління фінансово-економічною безпекою

Випускна кваліфікаційна робота

Виконала студентка групи
МФЕБм-21
А. А. Якобчук
_____

Науковий керівник:
к.е.н., доцент О. В. Баранецька
_____

Випускну кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **Н. Б. Москалюк**

ш20
29.11.19

ТЕРНОПІЛЬ - 2019

ЗМІСТ

ВСТУП …….. 3
РОЗДІЛ 1. КОНЦЕПТУАЛЬНІ ЗАСАДИ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Кіберзлочинність: генеза, сутність, види та наслідки…….. 7

1.2. Характеристика інформаційних злочинів в банківській сфері…… 16

ВИСОВКИ ДО РОЗДІЛУ 1…….. 32

РОЗДІЛ 2. АНАЛІЗ ДІЮЧОЇ ПРАКТИКИ БОРОТЬБИ З КІБЕРЗЛОЧИНАМИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

2.1. Нормативно-правове й інституційно-організаційне забезпечення протидії кіберзлочиннам в банківській сфері…….. 34

2.2. Аналітична характеристика кіберзлочинності у банківській сфері. 43

2.3. Напрями протидії інформаційним злочинам у банківській сфері.. 52
ВИСНОВКИ ДО РОЗДІЛУ 2…… 65

РОЗДІЛ 3. ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗЛОЧИНАМ У БАНКІВСЬКІЙ СФЕРІ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

3.1. Проблемні аспекти протидії кіберзлочинам у банківському секторі та можливі шляхи їх вирішення…….. 67

3.2. Міжнародний досвід попередження та запобігання кіберзлочинам у банківській діяльності і можливості його впровадження в Україні……. 77

ВИСНОВКИ ДО РОЗДІЛУ 3…… 90

ВИСНОВКИ…… 92

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……... 98

ВСТУП

Актуальність теми дослідження. У сучасних тенденціях розвитку світової економіки спостерігається активізація економічної злочинної діяльності. Процес глобалізації вивів її на якісно новий рівень, багаторазово ускладнивши і розширивши наповнення даної дефініції. Однією зі складових багатогранного поняття економічної злочинності є кіберзлочинність, що стала негативним наслідком розвитку інформаційних технологій.

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, що мають місце в електронному банківському обслуговуванні як у світі, так і в Україні. Результатом такої значної кількості кіберзлочинів через системи електронного банкінгу є зниження довіри громадян до надійності фінансової системи, банківських установ, 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.

Таким чином, проведення дослідження щодо протидії кіберзлочинам на сьогодні є необхідним та актуальним.

Огляд літератури з теми дослідження. Проблематикою кібершахрайств у банківській сфері займаються останні 10 – 15 років, що пов'язано із зростанням науково-технічного прогресу в галузі інформаційних технологій та програмного забезпечення, а також із збільшенням доступності до інформації з боку звичайного користувача. Так, типологія суб'єктів фінансового шахрайства в комерційних банках досліджувалася в наукових працях Д. Козлова, Н. Подосенка, О. Саяпіна, А. Шевченка та інших. Способи новітніх шахрайських операцій в банківський сфері представлені в працях О. Кришевича, С. Поперешняка, С. Волкової, А. Клочко, А. Єременко та інших. Що стосується способів боротьби із шахрайствами у банках, то питаннями застосування сучасних методів математичного моделювання та автоматизованих інформаційних систем для вирішення питань кібербезпеки, займалися вітчизняні та закордонні фахівці: Балдін, Ю. Барташевська, С. Кривошапова, Г. Яровенко та інші.

Незважаючи на велику кількість праць у даній сфері, не проаналізовано наслідки для банківської системи в результаті кібершахрайств та відсутні конкретні рекомендації щодо удосконалення банківської системи кіберзахисту.

Мета і завдання дослідження. Метою даної роботи є дослідження особливостей протидії кіберзлочинності в банківській сфері. Для досягнення поставленої мети передбачено постановку, формулювання і розв'язання наступних **завдань:**

– визначити сутність, генезис, види та наслідки кіберзлочинності;

– розглянути найбільш поширені інформаційні злочини у банківській сфері;

– дослідити нормативно-правове й інституційно-організаційне забезпечення протидії кіберзлочинам у банківській сфері;

– проаналізувати особливості здійснення та оцінити рівень кіберзлочинності у вітчизняній банківській системі;

– визначити напрями протидії інформаційним злочинам у банківській сфері;

– розглянути проблемні аспекти протидії кіберзлочинам у банківському секторі та запропонувати шляхи щодо їх вирішення;

– розкрити та конкретизувати досвід зарубіжних банків у боротьбі із кіберзлочинністю та можливістю його впровадження у вітчизняну практику.

Об'єктом дослідження є заходи протидії кіберзлочинам у сфері банківської діяльності.

Предметом дослідження є система суспільних відносин у сфері регулювання боротьби із злочинністю.

Методи дослідження. Основними методами, що були використані у даному дослідженні є: історичний метод – використаний при вивченні основних етапів розвитку та формування загального уявлення про стан кіберзлочинності і заходів протидії їй. Порівняльно-правовий метод – для аналізу існуючих угод і договорів, нормативно-правових актів, що регулюють питання кібербезпеки в Україні та країнах зарубіжжя, а також системний метод, який дозволяє проаналізувати структуру основних органів, що займаються питаннями попередження кіберзлочинів і їх взаємодії в процесі протидії правопорушенням. Статистичний, зокрема метод статистичного порівняння був використаний при розгляді динаміки розвитку і збільшення числа кібератак, з метою виявлення основних тенденцій щодо злочиності у кіберпросторі.

Інформаційна база роботи. Статистичну і фактологічну основу дослідження складають Закони України, нормативні документи Національного банку України, банківських установ, періодичні та монографічні наукові праці вітчизняних та зарубіжних науковців.

Наукова новизна роботи полягає в теоретичному обґрунтуванні та розробці методичних і практичних рекомендацій щодо протидії кіберзлочинам у банківській дільності.

Найбільш суттєві результати дослідження, що виносяться на захист, полягають у наступному:

1) на основні опрацьованих літературних джерел доповнено визначення «кіберзлочиності» в частині отримання вигод. Під кіберзлочиністю розуміється дія, що здійснюється за допомогою персонального комп'ютера, мобільного пристрою або інших технічних засобів, пов'язаних між собою мережею Інтернет, що порушує права людини, а також законодавчо встановлені норми, з метою отримання економічних, політичних, культурних та інших вигод;

2) здійснено аналіз основних видів кіберзлочинів у банківській діяльності в динаміці, а також визначені основні тенденції до зміни векторів правопорушень в сфері інформаційного середовища;

3) досліджено тенденцію розвитку правових норм міжнародної спільноти з протидії кіберзлочинності на міжнародному рівні та внесено пропозиції щодо вдосконалення законодавства у сфері правового регулювання боротьби із кіберзлочинністю у банківській сфері.

Практичне значення роботи. Практична значимість даного дослідження полягає в тому, що основні положення роботи щодо тенденцій розвитку кіберзлочинності і заходів боротьби з нею як на міжнародному так і на національному рівнях можуть бути використані для вдосконалення заходів протидії кіберзлочинам у банківській діяльності в рамках існуючих законодавчих і декларативних норм.

Апробація результатів роботи. Основні положення та результати роботи доповідались і обговорювались на Всеукраїнській науково-практичній конференції: «Економічна безпека: детермінанти та механізми забезпечення» (м. Тернопіль, ТНЕУ, 5 – 6 квітня 2019 р.).

Структура роботи. Випускна кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 108 сторінок, основний зміст викладено на 91 сторінці. Випускна кваліфікаційна робота містить 5 таблиць, 20

рисунків на 25 сторінках, список використаних джерел включає 110 найменувань та викладений на 10 сторінках.

РОЗДІЛ 1
КОНЦЕПТУАЛЬНІ ЗАСАДИ КІБЕРЗЛОЧИННОСТІ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1. Кіберзлочинність: генеза, сутність, види та наслідки

Стрімкий розвиток комп'ютерних технологій у різних сферах людського життя породив нові форми злочинної діяльності. У 60-ті роки XX століття комп'ютери використувалися в основному у військових і наукових цілях, а головною небезпекою був витік секретної інформації. У наступне десятиліття розвивалася економічна злочинність у сфері комп'ютерних технологій, а саме зломи банківських систем, промисловий шпіонаж. У 80-х роках були поширені зломи і незаконне поширення комп'ютерних програм. На початку становлення кіберзлочинності основною метою зловмисника було особисте збагачення, а комп'ютер використовувався як інструмент розкрадання, у 90-х роках XX століття основною метою кіберзлочинів став «інтелектуальний виклик», тобто прагнення показати свою перевагу в знанні комп'ютерних систем і засобів їх захисту. В даний час злочини з використанням комп'ютерних технологій часто стають інструментом незаконного політичного тиску та економічних злочинів. Крім того, інтеграція телекомунікаційних мереж, постійне вдосконалення пристроїв доступу до мережі створюють нові можливості для злочинів у сфері IT-технологій.

Масштабна хакерська атака з боку Росії проти України у 2017 року з використанням різновиду вірусу Petya спричинила порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок

атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низка інших великих підприємств. Зараженню піддалися інформаційні системи Міністерства інфраструктури, Кабінету Міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України.

За даними компанії ESET, яка розробляє програмне забезпечення для боротьби зі шкідливими комп'ютерними програмами, на Україну припало найбільше атак вірусу Petya — 75,24 % від усіх атак. Даний вірус атакував Німеччину (9,06 % атак), Польщу (5,81 %), Сербію (2,87 %), Грецію (1,39 %), Румунію (1,02 %), а також менш одного відсотка від всіх атак вірусу припало на Росію й Чехію [47].

За даними Німецького федерального агентства з безпеки інформаційних технологій (нім. Bundesamt für Sicherheit in der Informationstechnik, BSI) від атаки хробаком Petya постраждало одне німецьке підприємство, виробництво на якому зупинилось більше, ніж на тиждень. Зупинка виробництва потягнула за собою «мільйонні» збитки [47].

Експерт із інформаційної безпеки та протидії кіберзагрозам Віталій Якушев оцінив збитки підприємств по всьому світу від хакерської атаки у 8 млрд. доларів [68].

Як видно, комп'ютерне втручання може використовуватися не тільки для заподіяння шкоди економічним інтересам або безпеці країни, а також використовуватися в якості способу дестабілізації ситуації в суспільстві і навіть провокації неконституційних політичних процесів.

В Україні проблема боротьби із кіберзлочинністю ускладнена тим, що сам термін в нормативних та законодавчих документах не визначено, навіть не зважаючи на те, що поняття є звичним як для лексикону правоохоронних органів України і держав світу, так і для правової доктрини. Застосування сучасних інформаційних технологій практично в усіх сферах суспільного життя, у тому числі державних і недержавних структурах, висуває проблему

боротьби з кіберзлочинністю у число основних. Виникнення даного виду злочину вимагає введення спеціальної термінології. Однак до сих пір як в національних законодавчих актах так і в міжнародних договорах не має чіткого визначення дефініції «кіберзлочинність».

Поняття «кіберзлочини» нерідко виступає синонімом понять «комп'ютерні злочини» і «злочин в сфері комп'ютерної інформації», оскільки всіх їх об'єднує одне – це використання засобів комп'ютерної техніки для скоєння злочину, проте між ними існують істотні відмінності.

Слід зазначити, що комп'ютерні злочини і кіберзлочини деякі вчені трактують як різні види (групи) злочинів у сфері високих комп'ютерних технологій, класифікація яких здійснюється за різними ознаками. При цьому ознакою для «віднесення» окремих злочинів у сфері високих технологій до комп'ютерних в загальному вигляді є знаряддя скоєння злочину – комп'ютерна техніка, а ознакою для виділення кіберзлочину–специфічне середовище злочинів – кіберпростір (комп'ютерні системи і мережі) [8, с.249].

У вітчизняній літературі перевага віддається терміну «комп'ютерна злочинність», оскільки дослідження переважно ведуться в криміналістичній або процесуальній областях без урахування кримінологічного аспекту. Так, на думку Ю. М. Батурина, групи «кіберзлочинів» не існує. Він вважає, що «у зв'язку з використанням електронно-обчислювальних технологій більшість традиційних видів злочинів модифікувались, а тому більш правильно говорити лише про кібернетичні аспекти злочинів і не виділяти їх в відокремлену групу» [2, с. 129].

В науковій літературі закріпилася думка, що термін «комп'ютерний злочин» набагато ширше поняття «злочин у сфері комп'ютерної інформації». Ця думка базується на тому, що об'єктом комп'ютерного злочину можуть бути не тільки відносини, що складаються в сфері нормального обороту комп'ютерної інформації, а й інші суспільні відносини, які охороняються

законом, такі як відносини власності, честі, гідності, ділової репутації, громадський порядок, навіть світ і безпека людства.

Визначення поняття кіберзлочинності на теоретичному рівні включає в себе різного роду діяння, в яких інформаційно-телекомунікаційні системи або комп'ютерна техніка виступають в якості засобу вчинення злочину, або окреслюють коло кіберзлочинів, виходячи з предмету злочину або сфери суспільних відносин, в тому числі із зазначенням об'єкта або предмета злочинного впливу. Розглянемо їх більш детально.

Так, П. Д. Біленчук і Н. А. Зубань розглядають комп'ютерні злочини як суспільно небезпечну дію або бездіяльність, що здійснюється з використанням сучасних технологій і засобів комп'ютерної техніки, з метою заподіяння шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадських організацій і громадян, а також прав особи [5, с.16] .

В. Н. Бутузов до комп'ютерної злочинності відносить злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, визначаючи їх як посягання на відносини в сфері комп'ютерної обробки інформації, на право власності фізичних і юридичних осіб на інформацію та доступ до неї [9] .

Отже, терміни «кіберзлочинність» та «комп'ютерні злочини» дуже близькі за змістом, але все-таки помилково вважати їх синонімами. Термін «кіберзлочин» охоплює весь спектр злочинних діянь в IT-сфері: це і злочини скоєні за допомогою комп'ютерів, і злочини, предметом яких є комп'ютерні системи, мережі, де зберігається вся інформація. У той час комп'ютерні злочини – це тільки злочинні діяння, що посягають на безпечне функціонування комп'ютерів і комп'ютерних мереж, а також на оброблювані ними дані [4, с. 414]. Таким чином, поняття «кіберзлочинність» ширше, ніж «комп'ютерна злочинність », і більш точно відображає природу такого явища, як злочинність в інформаційному просторі.

Наприклад, Т. Л. Тропіна в своїх роботах використовує термін «кіберзлочини», під яким розуміє злочинність в так званому «віртуальному просторі» [71, с.48]. Віртуальний простір автор визначає як «змодельований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному чи будь-якому іншому вигляді і знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі «...». Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, скоєний в електронному середовищі» [71, с.49].

Дане визначення, на наш погляд, розкриває природу злочину, вчиненого з використанням комп'ютерних засобів, проте є занадто широким і неточним. Так, можна припустити, що під «інші суспільно небезпечні діяння, вчинені за допомогою комп'ютера» можуть потрапляти і такі злочини, в яких комп'ютер був застосований не за своїм основним призначенням, наприклад, в разі якщо комп'ютером було завдано удару іншій людині. При цьому в таких злочинах різна ступінь використання комп'ютера, різні способи вчинення злочину, різні об'єкти і предмети посягання, і, як наслідок – інші характер і ступінь суспільної небезпеки.

І. М. Россолів ототожнює поняття «кіберзлочини» і «комп'ютерні злочин», і визначає його наступним чином: «Головною особливістю кіберзлочину (комп'ютерного злочину, злочину в сфері високих технологій) є використання мереж комп'ютера для здійснення протиправного вчинку або злочину у віртуальному просторі «...» до кіберзлочинів відносяться такі суспільно небезпечні діяння, які відбуваються з використанням засобів комп'ютерної техніки щодо інформації, яка обробляється і використовується в Інтернеті» [88].

На нашу думку, дане визначення є занадто вузьким, оскільки, по-перше, існують і інші інформаційно-телекомунікаційні мережі, що

утворюють кіберпростір, крім мережі «Інтернет» («FidoNet» або будь-які приватні локальні мережі); по-друге, в кіберпросторі скоюються злочини у відношенні не тільки інформації, але і власності, а також інших суспільних відносин (суспільної безпеки, суспільної моралі).

Крім розглянутих найбільш поширених термінів, деякими авторами використовуються власні поняття: «злочини у сфері інформаційних технологій», «злочини вчинені в кіберпросторі», «злочини в сфері високих технологій» та інші.

І. Г. Чекунов, наприклад, вводить термін «злочини, що здійснюються з використанням комп'ютерних мереж». Він пише: «в теорії кримінального права та кримінології домінують точки зору, згідно з якими комп'ютерні злочини утворюють злочинні діяння, пов'язані з несанкціонованим доступом до мереж, серверів, машинних ресурсів, і, як правило, орієнтовані на пошкодження або знищення інформації, порушення нормального стану комп'ютерів або комп'ютерних мереж. Нами ж система злочинів, скоєних з використанням комп'ютерних мереж, розглядається в більш широкому сенсі і включає в себе злочинні діяння, в тому числі пов'язані і з санкціонованим доступом до серверів і комп'ютерних мереж» [102, с.178].

В. Г. Степанов-Егіянц поряд з терміном «комп'ютерні злочини» застосовує термін «злочини з використанням комп'ютерної техніки». Не даючи визначення, автор лише зазначає, що «найбільш поширеними злочинами з використанням комп'ютерної техніки є: хакерство, комп'ютерне шахрайство, поширення шкідливих програм, комп'ютерне піратство».

І. М. Соловйов використовує термін «злочин, скоєний в кіберпросторі». Згідно його точки зору, це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, вчинені з допомогою або при допомозі комп'ютерів, комп'ютерних мереж і програм. Поняття «кіберзлочини» не обмежується рамками мережі Інтернет,

оскільки воно поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері.

У вітчизняній літературі термін «кіберзлочин» часто ототожнюється з такими термінами як «комп'ютерний злочин», «злочин у сфері комп'ютерної інформації», «злочин у сфері використання комп'ютерів», «злочин у сфері використання інформаційних технологій», або із законодавчим в Україні поняттям «злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Все це ставить під великий сумнів доцільність і можливість нормативного визначення кіберзлочину і впровадження його як окремого виду злочинів кримінальним кодексом України.

Відповідно до рекомендацій ООН, категорія «кіберзлочинність» має на увазі суспільно небезпечне діяння, яке може відбуватися за допомогою або в рамках компютерної системи або мережі, або проти них. Інакше кажучи, до кіберзлочинів відносяться злочинні посягання, які відбуваються в кіберпросторі за допомогою або засобом комп'ютерних систем або мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж і проти комп'ютерних систем, мереж і даних [13, с.277].

Виходячи з вищевикладеного можна визначити «кіберзлочинність» як сукупність суспільно небезпечних діянь, що вчиняються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, компютерних мереж і комп'ютерних даних. Дане визначення охоплює всі види злочинів в IT-сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть стати предметом, засобом або знаряддям злочинних посягань, а також середовищем, в якому відбуваються правопорушення.

Крім того, важливо відзначити ряд особливостей, які характерні для більшості кіберзлочинів:

 кіберзлочинці досягають своїх цілей за рахунок неправомірного використання ІТ-технологій;

 транскордонність, тобто такі протиправні діяння відбуваються в законодавчо неврегульованому, безмежному, віртуальному кіберпросторі з виходом за національні кордони;

 активна динаміка використання високих технологій та передових наукових досягнень, а саме: складність, різноманіття, нестандартність способів скоєння злочинів із застосовуванням спеціальних засобів, що безпосередньо залежить від зростання кількості і якості технічних можливостей комп'ютерів, вдосконалення їх програмного забезпечення, розширення комп'ютерних мереж;

 як правило, потерпілі не інформовані про те, що вони піддалися злочинному впливу;

 злочинні дії відбуваються дистанційно, в умовах відсутності фізичного контакту злочинця і потерпілого;

 кіберзлочини мають високу латентність. За різними оцінками, латентність кіберзлочинів становить в США – 80%, у Великобританії – 85%, в Німеччині – 75%, в РФ – 90% [7, с. 87];

 масштабність правопорушень, або іншими словами, можливість використання десятків і навіть сотень тисяч комп'ютерів, в програмне забезпечення яких «впроваджена» розгалужена «бот-мережа»;

 в основному кіберзлочини здійснюються з корисливих мотивів. Однак умисел може бути спрямований на досягнення інших цілей, наприклад, політичних;

 суб'єкт кіберзлочину, як правило, інтелектуально-розвинений і високопрофесійний фахівець в сфері ІТ-технологій;

 існування стійкої і зростаючої тенденції до «організованості» кіберзлочинності, до групового характеру скоєння таких правопорушень.

Отже, кіберзлочинність – це складне, багатопланове явище, яке становить загрозу для безпеки міжнародного співтовариства, держави,

суспільства, індивіда. Небезпека кіберзлочинів полягає в їх нестандартному, трансграничному, організованому характері, що в свою чергу веде до складнощів, пов'язаних з попередженням, припиненням та розслідуванням злочинів даного виду традиційними засобами.

Таким чином, під кіберзлочинністю слід розуміти відносно масове соціально-правове явище, яке охоплює сукупність суспільно небезпечних діянь, передбачених КК України, Конвенцією про кіберзлочинність та Додатковим протоколом до неї з урахуванням застережень, прийнятих Верховною Радою України, в яких інформаційно-телекомунікаційна система або її елементи є засобом вчинення злочину.

За останні п'ять років в Україні кількість інформаційних злочинів зросла мінімум в 2,5 рази [17].

Стрибок числа всіх кіберзлочинів відбувся в 2017 році. Після цього кількість злочинів має тенденцію зростати. Так в 2017 році було зафіксовано 1795 справ, в 2018 – 1023, за останні півроку – 1005 (рис. 1.1).

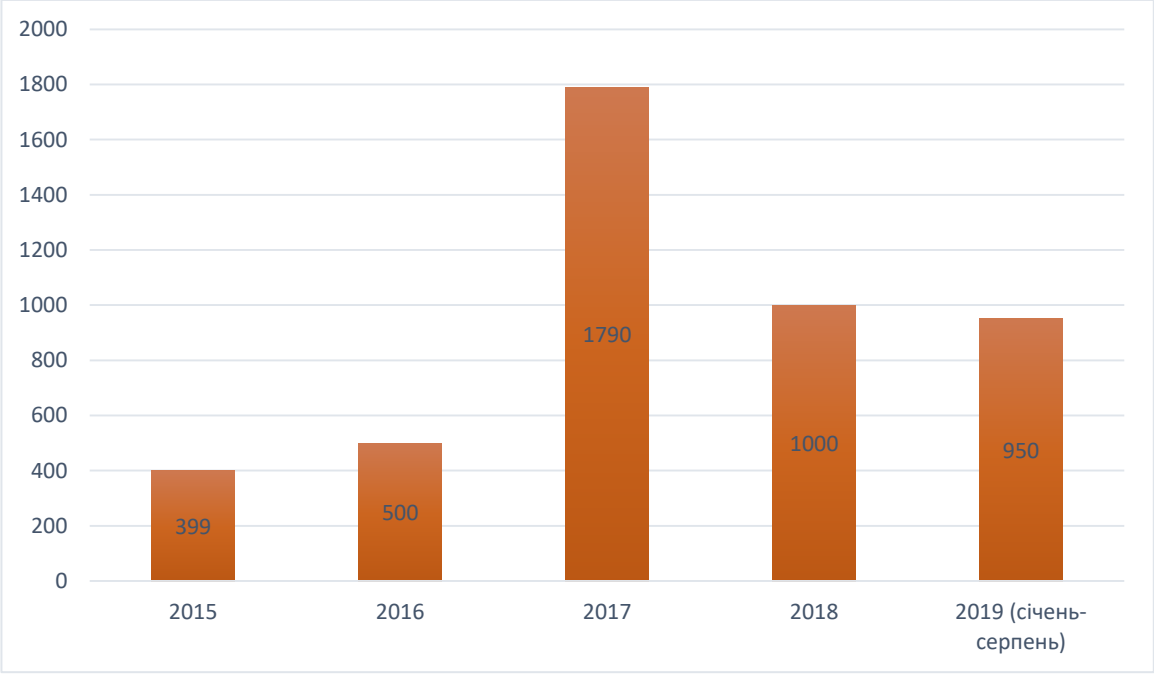

Рис. 1.1. Кількість здійснених кіберзлочинів в Україні протягом 2015-2019 рр. [17]

Стрибок кіберзлочинності у 2017 року значною мірою пов’язаний з вірусом «Петя», який вразив тисячі компаній, однак тоді заяви в кіберполіції про дані, втрачені через цей вірусу, часто залишалися без відповідей.

Разом з цим, статистичні показники не відображають реальної картини кіберзлочинності, тому що не враховують: комп’ютерне шахрайство (ст. 8 Конвенції), злочини, пов’язані з дитячою порнографією (ст. 9 Конвенції), порушення, пов’язані з порушеннями авторського права і суміжних прав (ст. 10 Конвенції), а також можливість здійснення «традиційних» злочинів з використанням інформційно-телекомунікаційних мереж. Згідно з дослідженнями, проведеними американським Центром стратегічних і міжнародних досліджень та компанією McAfee, щорічні втрати світової економіки від кіберзлочинів досягли вже 500 мільярдів доларів [17] .

Отже, зважаючи на вищезазначене, можна дійти висновку, що кіберзлочинність стала проблемою саме XXI ст. у зв’язку із жвавою модернізацією технологій та суспільства, і з кожним роком кількість кіберзлочинів, які поглинають все більше коштів, зростає. Звичайно, вживаються заходи щодо протидії такому виду злочинності, але їх недостатньо, тому потрібно розробляти нові методи боротьби, що дадуть набагато більше позитивних результатів, а також покращити або розробити системи захисту, які допоможуть уникнути або мінімізувати такі види злочинів. Сьогодні кібербезпека в Україні є на дуже низькому рівні, а тому не варто нехтувати таким важливим чинником, як безпека в інтернет-просторі, оскільки в багатьох країнах світу цей напрям є пріоритетним як у врутрішній так і у зовнішній політиці.

1.2. Характеристика інформаційних злочинів у банківській сфері

Стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп’ютерних технологій з корисливих та інших мотивів, що певною мірою ставить під загрозу національну безпеку держави.

Разом з поширенням впровадження сучасних інформаційних технологій в Україні постійно зростає загроза як для державних комп'ютерних систем, так і для приватних організацій та окремих громадян. Особливої актуальності проблема кіберзлочинності набула в наш час.

Соціологічні опитування в різних країнах, і насамперед у високорозвинених, показують, що кіберзлочинність посідає одне з чільних місць серед тих проблем, які турбують людей. Більше того, на думку фахівців, сьогодні це явище становить значно серйознішу небезпеку, ніж 5 років тому через використання зі злочинною метою новітніх інформаційних технологій, а також зростаючої уразливості сучасного індустріального суспільства. Незважаючи на зусилля держав, які спрямовані на боротьбу з кіберзлочинами, їх кількість у світі не зменшується, а, навпаки, постійно зростає [5, с. 17]. Саме тому, на даний момент назріла нагальна потреба у визначенні методів мінімізації інформаційних злочинів та злочинів у банківській діяльності зокрема.

Водночас тенденції розвитку суспільних відносин в Україні протягом останніх років демонструють такі найбільш поширені кіберзлочини: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем із метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини.

Кіберзлочини є п'ятим за розміром видом економічної злочинності після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю (рис. 1.2).

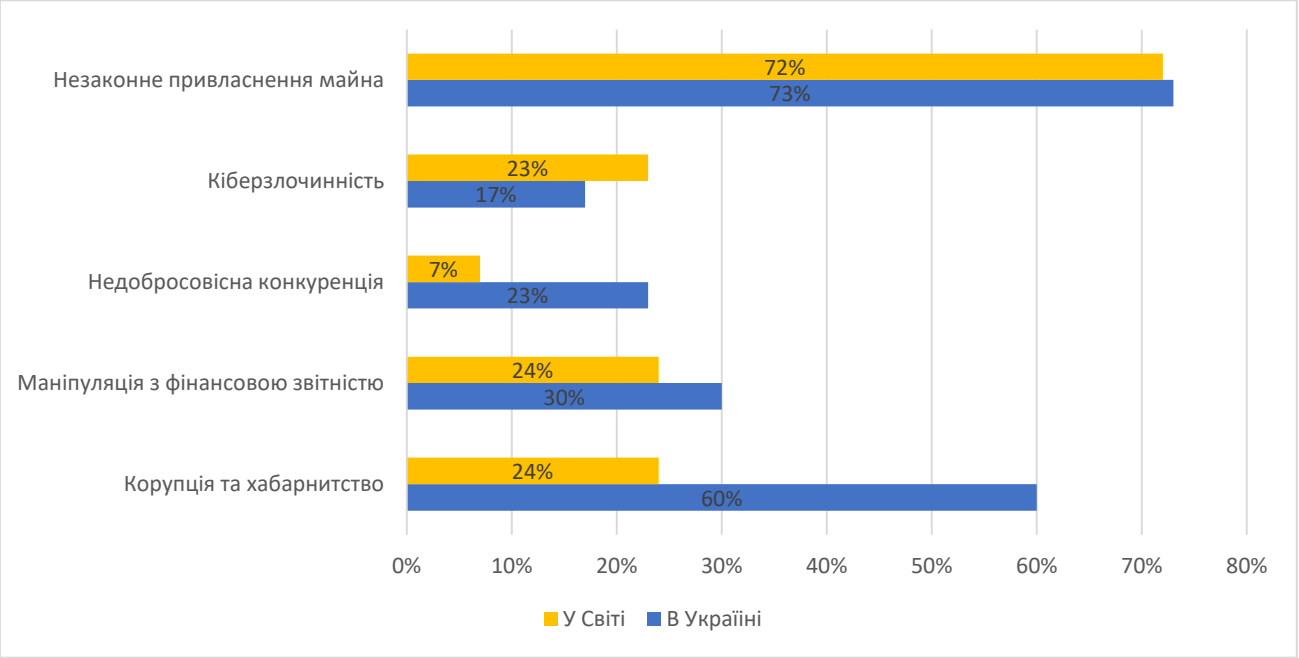

Рис. 1.2. Найпоширеніші економічні злочини в Україні та світі [11, с. 358]

Але основним об'єктом шахрайства є ресурси банківських установ. Окрім того, комп'ютерних атак на банківську систему насправді набагато більше, ніж свідчить офіційна статистика. Це пояснюється тим, що багато з кібератак є невдалими, а виявлені прогалини в системі електронного банкінгу швидко відновлюються. Інформація про діяльність кіберзлочинців у банку може вплинути на рівень довіри клієнтів до банківської установи. Як наслідок, клієнти банку можуть почати виводити банківські депозити з банків у масовому масштабі, що стане серйозною проблемою для банків, пов'язаною з різким зростанням рівня ризику ліквідності, тому достовірний обсяг кіберзлочинності оцінити достатньо важко.

Основні види кіберзлочинів, що здійснюються у банківській діяльності узагальнено в табл. 1.

За статистикою, найпоширенішим в Україні за кількістю підтверджених інцидентів є банкоматний скіммінг, який залишається основною загрозою для безпеки банкоматів внаслідок міграції скіммінгових пристроїв з Європи. В Україні переважає обіг карток з магнітною смугою, що приваблює шахраїв з усього світу. Так, правоохоронними органами за фактами встанов-

лення скіммінгових пристроїв на українських банкоматах неодноразово затримувались громадяни Китаю, Румунії, Болгарії та Молдови.

Основними видами Інтернет-шахрайств є:

- фішинг – вид Інтернет-шахрайства, направлений на отримання ідентифікаційних даних клієнтів (крадіжки паролів, номерів і даних кредитних карт, банківських рахунків та іншої конфіденційної інформації). Виділяють три основні види фітингу – поштовий, онлайновий і комбінований.

- телефонний фішинг – вид шахрайства, що передбачає отримання інформації про платіжну картку клієнта за допомоги телефонного дзвінка з проханням повідомити PIN-код, код CVV2/CVC2 чи іншу конфіденційну інформацію.

- комп’ютерні віруси, спрямовані на збір інформації про дані платіжних карт; комп’ютерні програми, особливістю яких є здатність збору інформації про дані платіжних карт, які зберігають/вводять на комп’ютер, заражений вірусом.

Таблиця 1.1

Основні види кіберзлочинів у банківській сфері

Характеристика	
ммінг (виготовлення, збут та встановлення на банкомати- ння/копіювання інформації з магнітної смуги платіжної ія ПШ-коду до неї); ілого пластику» для «клонування» (підробки) платіжної тівки в банкоматах; sal Fraud - втручання в роботу банкомату при здійсненні тівки, яке залишає незмінним баланс карткового рахунку риманні готівки зловмисником; заклеювання диспенсеру для привласнення зловмисником писана з карткового рахунку законного держателя картки.	-
вних угод торговельного еквайрінгу для обслуговування- кних карток; ізитів платіжних карток, у тому числі із застосуванням х «клонування»; нижче встановленого ліміту без проведення авторизації; ачених/викрадених/підроблених платіжних карток.	-
ютерних вірусів та троянських програм для прихованого- вління комп'ютером клієнта; ів, проведення несанкціонованих операцій та отримання і несанкціонованих операцій у системах ДБО; ежів від закордонних відправників через міжнародну наслідок втручання у роботу комп'ютерів та систем ДБО их банківських установ.	-
зитів платіжних карток; ацій із використанням викрадених реквізитів платіжних створення програмних засобів для викрадення реквізитів к (створення фіктивних WEB-сайтів, поширення сів та троянських програм, перехоплення трафіку тощо).	-
тів за підробленими документами; пового шахрайства з залученням у злочинні схеми , торгівельних мереж і правоохоронних органів; ід банківські правила та моделі скорингової оцінки сті позичальників; ердження працевлаштування і доходів.	-

У 2015 р. слід відзначити тенденцію щодо збільшення випадків кредитного шахрайства. За оцінками служб безпеки українських фінансових установ, рівень загрози від шахрайств за кредитними операціями на сьогодні

обчислюється мільярдами доларів. Для мінімізації кредитних шахрайств банкам необхідно вести облік відмов у кредиті, неповернень, прострочених платежів, випадків шахрайства, та узагальнювати дану інформацію, тісно співпрацюючи з зовнішніми базами даних, такими як Бюро кредитних історій.

Наслідками кіберзлочинів у банківській сфері є зниження довіри клієнтів до захисту персональних даних, до фінансових операцій, що проводяться з використанням новітніх технологій, і, як наслідок, до надійності фінансової системи в цілому. При цьому, недовіра клієнтів до ринків фінансових послуг перешкоджає активно використовувати вільні грошові кошти населення, як інвестиційні ресурси, що спрямовуються на розвиток банківської системи та економіки загалом.

Сьогодні основними джерелами ризику кіберзлочинів в умовах електронного банкінгу є операції, пов’язані з платіжними картками, обслуговування через банкомати, обслуговування в системі Інтернет-банкінгу, а також використання мобільних додатків для обслуговування через систему мобільного банкінгу. Тому, на нашу думку, для якісної ідентифікації ризику кіберзлочинів електронного банкінгу, його варто поділяти на 1) ризик шахрайства з платіжними картками; 2) ризик шахрайства з банкоматами; 3) ризик шахрайства з мобільним телефоном та Інтернетом (рис. 1.3).

Значна кількість банківських установ України надає перевагу подоланню наслідків кіберзлочинів, а не інвестуванню коштів у пошук засобів захисту даних та рахунків своїх клієнтів.

Вважаємо за потрібне більш детально розглянути кожен із видів кіберзлочинів для розуміння їх сутності та особливостей, якими вони характеризуються, що дасть змогу у подальшому їх вчасно ідентифікувати та розробити методи щодо їх попередження.

Кіберзлочини з платіжними картками є найпоширенішим видом шахрайства, що характеризується широким різновидом і кожного року

видозмінюються. Сьогодні виокремлюють до 10 видів шахрайств із платіжними картками, однак найбільш поширенішими є соціальна інженерія (вішинг, фішинг), фармінг, трешінг.

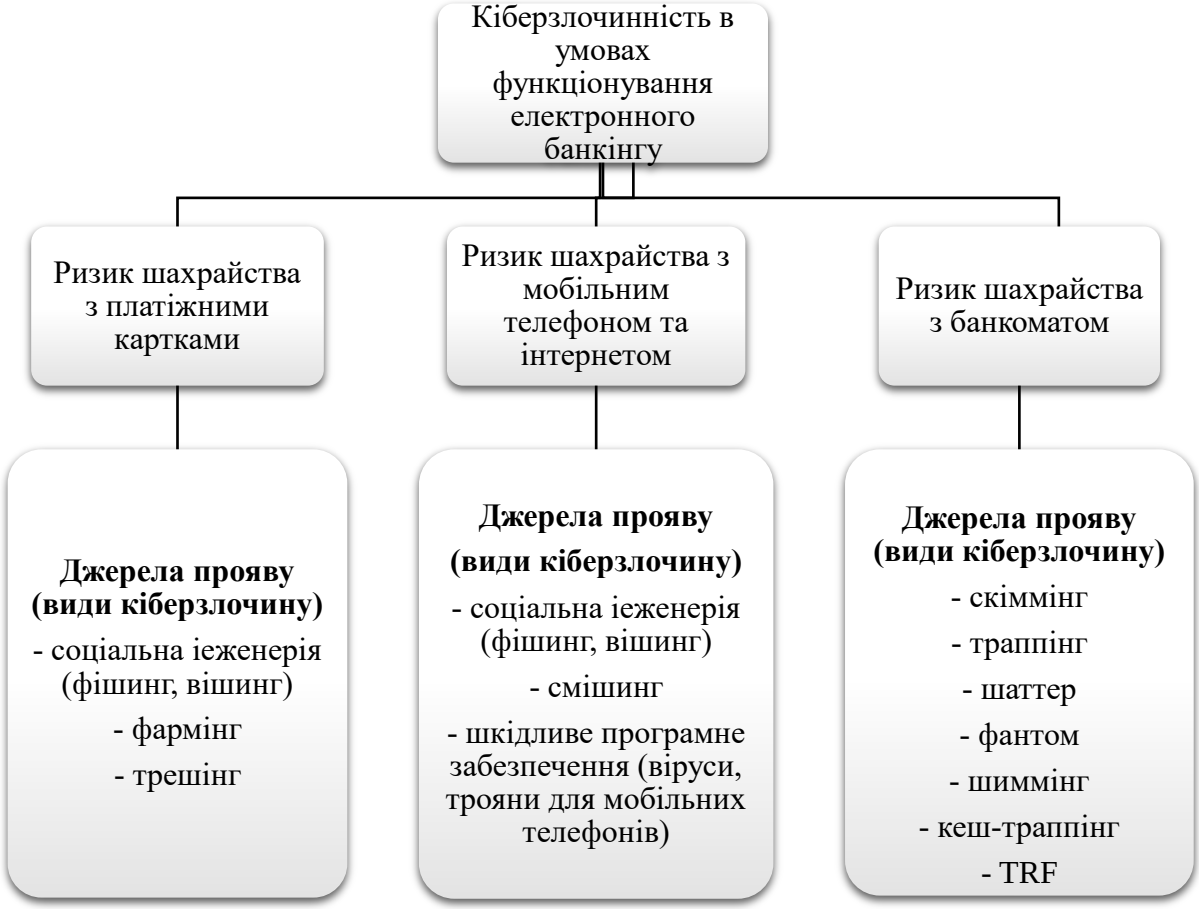

Рис. 1. 3. Класифікація кіберзлочинів в умовах електронного банкінгу [33, с.93]

Дослідження правоохоронних органів показали, що найбільш поширеним видом кіберзлочинів з використанням платіжних карток є злочини з використанням підроблених карок і вкрадених реквізитів діючих карток.

Можна виділити дві групи злочинів, що здійснюються з використанням платіжних карток: злочини, що здійснюються в системі банку та злочини, що здійснюються поза банком.

До першої групи злочинів відносяться: несанкціоноване встановлення на картку кредитного ліміту, що дозволяє збільшити авторизований залишок на картковому рахунку з наступним зняттям коштів; несанкціоноване

встановлення в авторизованій системі спеціального статусу рахунку, що дозволяє в певних межах знімати кошти з картки; випуск паралельної карти-двійника; несанкціонований випуск нових платіжних карт; змова з представниками торговельних точок та ін.

У групі злочинів, скоєних поза банком, можна виділити три групи злочинів: злочини, що здійснюються за участю власника платіжної карти; злочини, що здійснюються з використанням підроблених, вкрадених карток або ідентифікаційних даних; злочини пов'язані з несанкціонованим проникненням в сховища даних або шляхом проникнення в різні пристрої.

Злочини, вчинені з використанням підроблених, вкрадених карток і ідентифікаційних даних, можна розділити на наступні види:

1. Шахрайство з використанням вкрадених карт.

2. Шахрайство з використанням підроблених карток. Відповідно до даного виду злочину здійснюється розкрадання грошових коштів з рахунків законних власників. Кіберзлочини у даному випадку здійснюються за допомогою неправомірного доступу до серверів процесингових центрів банківських установ, де копіюється інформація про власників карток. Згодом дані надходять до організаторів, які за допомогою спеціального принтера виготовляють платіжні карти з магнітною смугою і логотипами банків, і за допомогою «енкодера», записують викрадену банківську інформацію на пластикові карти та знімають готівкові кошти.

3. Шахрайство з використанням карток з частковою підробкою [49, с.86].

4. «Білий пластик». При використанні даного способу на заготовках пластика стандартного розміру зловмисники ембосують номери дійсних платіжних карт. Магнітна смуга копіюється зі справжньою карти, наприклад за допомогою скімера. Щоб скористатися «Білим пластиком» шахраї вступають в змову з касирами торгового підприємства, нерідко для операцій з «білим пластиком» створюються підставні фірми. Так, у 2008 р злочинці дізналися про уразливе місце комп'ютерного захисту компанії PBS WorldPay,

яка займається оформленням платежів, в тому числі по кредитних і дебетових картках, і є підрозділом Royal Bank of Scotland. Об'єктом злому стали дебетові карти, прив'язані до рахунків, на які роботодавці перераховували заробітну плату своїм співробітників. В результаті такого кіберзлочину банківська установа понесла мільйоні збитки [54, с.117].

5. Шахрайство торгової точки. Суть даного виду злочину проявляється у співпраці касира магазину та кіберзлочинця, який за допомогою спеціальних пристроїв, зчитуючи інформацію з POS-терміналів, знімає готівку із платстикових карток покупців.

6. Шахрайство з використанням номера рахунку. Проникаючи у мережі, зловмисники отримують повну інформацію про номери дійсних платіжних карток, терміни їх дії та імена власників. Використовуючи ці дані, кіберзлочинці переводять ці кошти на рахунок віртуального магазину або фірми. Потім під приводом відмови від покупки оформляється повернення електронних грошей на рахунок злочинця, після чого гроші легко переводяться в готівку.

7. Копіювання магнітної смуги (Скімінг). Даний вид шахрайства передбачає використання особливих видів пристроїв, що зчитують інформацію з магнітних смуг карток. Скіммер зчитує і записує інформацію на магнітній смузі. Тобто у зловмисників з'являється дані необхідні для подальшого виготовлення підробленої карти і її використання в своїх цілях.

8. Фішинг, вид шахрайства в результаті якого зловмисникам шляхом обману стають доступні реквізити банківської картки і пін-код. Найчастіше використовується у вигляді розсилки через Інтернет листів від імені банку або платіжної системи з проханням підтвердити зазначену конфіденційну інформацію на сайті організації. В Україні почастішали випадки появи web-сайтів, на яких пропонуються різні фінансові послуги з використанням платіжних (банківських) карток міжнародних платіжних систем, таких як VISA і MasterCard. Користувачам пропонується заповнити електронні форми і вказати реквізити платіжних (банківських) карток, включаючи пін-код. При

цьому передача конфіденційної інформації ведеться без використання захищених протоколів інформаційного обміну [62, с.90].

Станом на 01.10.2017 року кількість фішингових сайтів становила 84 шт. (рис. 1.4), а з початку 2017 року спостерігається тенденція до їх збільшення, однак найбільш піковим роком розвитку шахрайства за допомогою фішингових сайтів був 2016 рік. Згідно з даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2016-му кожен сотий власник платіжної картки в Україні став жертвою шахраїв, а загальні втрати становили майже 340 млн. грн. [7].

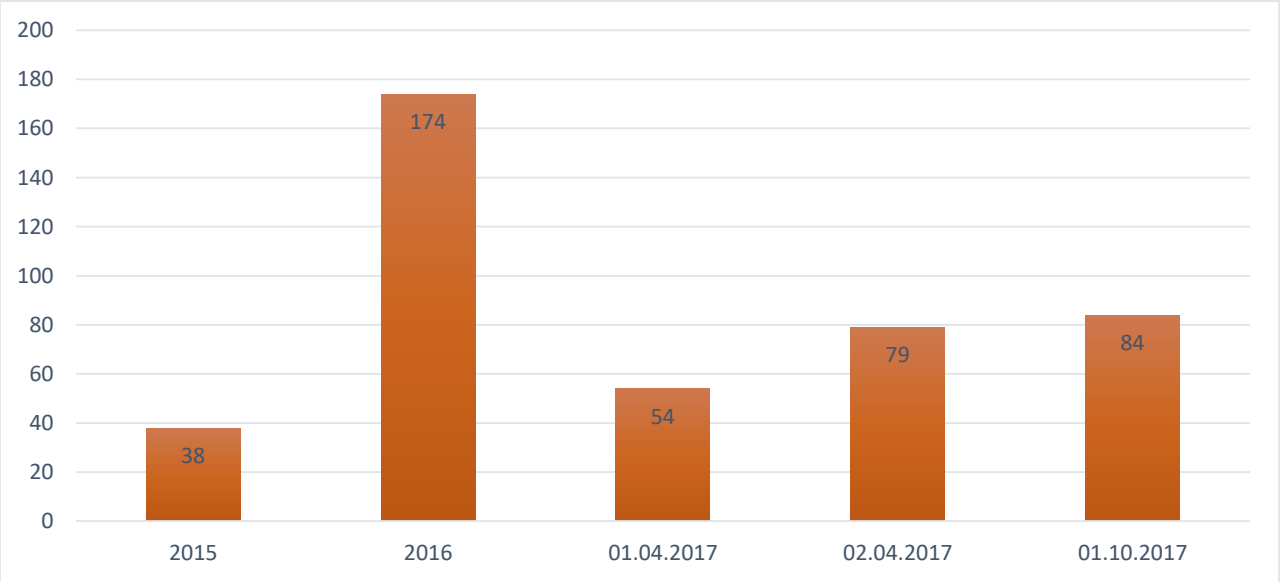

Рис. 1.4. Кількість виявлених фішингових сайтів у 2015–2017 рр. [33, с.94]

Відповідно до статистичних досліджень системи міжбанківського обміну інформацією Exchange-Online, у 2016 році 95% фішингових сайтів були спрямовані на отримання реквізитів платіжних карток, пропонуючи неіснуючу послугу для переказу з картки на картку та поповнення мобільного.

У І кварталі 2018 року основний профіль фішингових сайтів розширився, як видно на рис. 1.5, фішингові сайти імітують не тільки сервіси для грошових переказів та поповнення мобільного телефону, але й сайти для покупки авіаквитків (рис. 1.5).

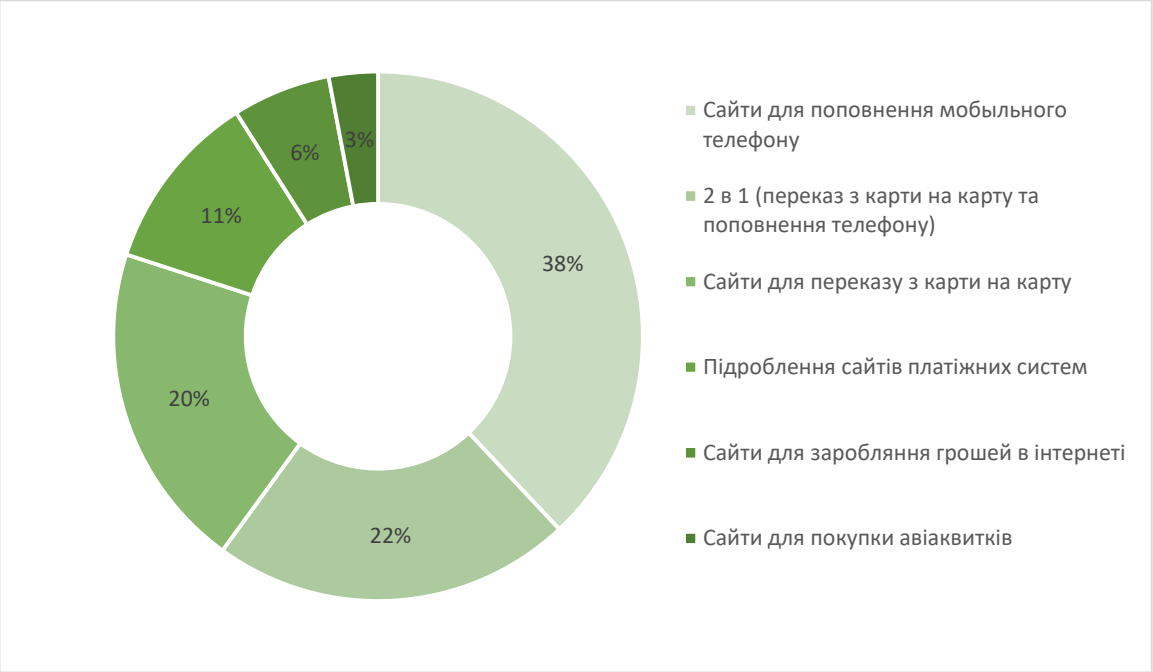

Рис. 1.5. Різновиди фішингових сайтів станом на 1 квартал 2018 р. [33, с.95]

За даними асоціації ЄМА, за місяць роботи один фішинговий сайт відвідують від 15 до 30 тис. користувачів, що є негативним та вказує на високий рівень необізнаності користувачів платіжних карток про фішингові кіберзлочини.

9. Вішинг, або голосовий фішинг, вид шахрайства, при якому зловмисник використовує технологію, що дозволяє автоматично збирати інформацію про реквізити діючих карток, при якому зловмисники імітують дзвінок автоінформатора, який повідомляє, що з його карткою здійснюються шахрайські дії і дає інструкції - передзвонити за певним номером. Зловмисник, що приймає дзвінки за вказаним автовідповідачем номером, представляється співробітником банку і просить провести звірку, під час якої і отримує всі необхідні дані.

Вішинг виник у середині 2006 року, однак в Україні він набрав обертів лише в 2015 році. З цим видом шахрайства у 2015 році зіткнувся кожен 220-й українець, а 2016 році – вже кожний 80-й житель України. Внаслідок вішингу у 2016 році з рахунків українців було вкрадено 275,45 млн. грн.

(або 81% від загальних втрат шахрайства з платіжними картками) проти 51,74 млн. грн. в 2015 році [33, с.95]. Середня сума вішингових операцій у 2015 році становила 834 грн., а у 2016 році – вже 1403 грн [17]. Найчастіше жертвами вішингу стають люди пенсійного віку, а саме користувачі пенсійних проектів банківських установ, оскільки їхня необізнаність та високий рівень довіри до людей робить їх особливо вразливими до цього виду злочину. Відповідно до досліджень асоціації ЄМА 76% осіб, до яких телефонували шахраї, стали жертвами вішингу (надали реквізити платіжної картки) [17].

Іншим видом злочину з платіжними картками є фармінг, який, як і вішинг, є різновидом фішингу. Особливістю цього виду шахрайства є те, що фармінг-технології дають змогу змінити IP-адресу сайту і під час входу на web-сторінку легітимної організації проводиться перенаправлення на підроблену, яка створена для збору конфіденційної інформації. Найчастіше такі сторінки підмінюють сторінки банків. Фармінг здійснюється двома способами: 1) на комп'ютер хакерами встановлюється шкідливе програмне забезпечення, яке автоматично перенаправляє користувача на нелегітимний сайт для викрадення конфіденційної інформації; 2) хакери вражають вірусами сервер DNC (сервіс доменів сайтів), у результаті чого кожен відвідувач відповідного сайту автоматично буде переправлений на сайт шахраїв. Цей вид шахрайства дуже складно розпізнати, оскільки підроблений сайт роблять висококваліфіковані фахівці і його дуже важко розпізнати [74, с.92].

Варто відзначити, що під час фішингу та вішингу жертва під впливом психологічних методів та неуважності стає жертвою шахраїв, а під час фармінгу шахрай не контактує з жертвою. Найпростішим методом захисту від фармінгу є встановлення на персональний комп'ютер офіційного антивірусу.

Загалом, у банківській практиці виділяють ще одну групу кіберзлочинів – це шахрайство з мобільним телефоном та Інтернетом, тобто в цю групу

віднесено всі види шахрайства, для реалізації яких використовується мобільний телефон та мережа Інтернет.

Європейські та американські банки, а також платіжні системи пропонують різні способи захисту фінансових операцій користувачів, у тому числі перевірку справжності користувача з використанням USB-токенів, одноразових паролів, підтвердження операцій за допомогою кодів, що відправляються на телефон. Проте кіберзлочинці розробляють програми, які дають змогу обходити ці захисні заходи.

Як відомо, смартфони працюють на одній із трьох платформ – iOS, Android і Windows Phone. Найбільш поширеною платформою є Android, її частка на ринку становить 70%. За інформацією «Лабораторії Касперського», 99% шкідливого програмного забезпечення для мобільних телефонів націлені саме на платформу Android, і в середньому кожного року створюється понад 35 тис. шкідливих програм, які спрямовані на викрадення приватної інформації власника смартфону, в тому числі і паролів для входу в систему Інтернет- банкінгу чи мобільного банкінгу [9].

ТОП-10 країн за часткою користувачів, які були атаковані мобільним «банківським троянцями» представлена в табл. 1.2.

Таблиця 1.2

ТОП-10 країн за часткою користувачів, які були атаковані мобільним «банківським троянцями» [33, с.96]

Країна	**Частка атакованих користувачів, % 3 кв. 2017 року**	**Країна**	**Частка атакованих користувачів, % 2 кв. 2018 року**
Росія	3,12	Росія	1,63
Австралія	1,42	Австралія	0,81
Україна	0,95	Туреччина	0,81
Узбекистан	0,60	Таджикистан	0,44
Таджикистан	0,56	Узбекистан	0,44
Казахстан	0,51	Україна	0,41
Китай	0,49	Латвія	0,38
Латвія	0,47	Киргизстан	0,34
Корея	0,41	Молдавія	0,34
Білорусія	0,37	Казахстан	0,32

Частка атакованих українських користувачів є незначною і в другому

кварталі 2018 року скоротилася, однак Україна все ще входить в десятку країн, жителі якої найчастіше атаковані шкідливими програмами для смартфонів.

Остання група, яка провокує появу ризику шахрайства в умовах функціонування електронного банкінгу, є шахрайство через банкомати. Обсяг шахрайства через банкомати в Україні йде на спад, однак залишається вагомим. Основні види шахрайства через банкомат представлені в табл. 1.3.

Таблиця 1.3

Основні види шахрайства через банкомати [33, с.96]

№	Вид	Характеристика
1.	Скіммінг	Вид шахрайства для отримання реквізитів платіжної картки, що здійснюється за допомогою спеціального засобу, який встановлюється на банкомат,– скімера, який зчитує номер та пін-код картки. Після отримання необхідної інформації картка дублюється і гроші міняють власника за лічені хвилини.
2.	Треппінг	Вид шахрайства через банкомат, що здійснюється за допомогою «ліванської петлі», яка виготовляється з фотоплівки та встановлюється на картрідер банкомату. Потім жертва підходить до банкомату, вставляє картку, отримує гроші, але картка не повертається.
3.	Фантом	Найбільш дорогий та технічно складний вид шахрайства з банкоматом. Його суть полягає в тому, що шахраї встановлюють муляж банкомату, який виглядає як справжній банкомат, що обладнаний спеціальними пристроями, які зчитують інформацію з картки.
4.	Шаттер	Вид шахрайства, за якого на шаттер (проріз, через який відбувається видача грошей) наклеюється сторонній пристрій, що блокує видачу купюр банкоматом власнику картки. Відбувається це за рахунок розміщення липкої стрічки на внутрішній частині пристрою, до якої і пристають купюри. Відповідно, цей пристрій не дозволяє банкомату ні забрати кошти назад, ні видати їх власнику, в результаті згодом їх забирає шахрай.
5.	Шиммінг	Один зі способів незаконного зняття грошей за допомогою використання тонкої плівочки, схожої на скоч. Така плівка наклеюється на клавіатуру банкомата, а потім із неї зчитується необхідна інформація. Незвичайна клавіатура банкомата не викликає підозри, що значно полегшує завдання злочинцям.
6.	Кеш-треппінг	Вид шахрайства, що здійснюється за допомогою закриття отвору для видачі грошей в банкоматі спеціальної накладкою (планкою) з липкою стрічкою зі зворотного боку. Таким чином, під час проведення громадянами операцій зі зняття готівки відбувається захоплення купюр (гроші прилипають до планки), що перешкоджає їх видачі законному власнику картки.

7.	TRF (Transaction Reversal Fraud – скасування операції)	Шахрайство через банкомат, що здійснюється шляхом втручання в роботу банкомату під час здійснення операцій видачі готівки, яке залишає незмінним баланс карткового рахунку за фактичного отримання готівки зловмисником.

Відповідно до опублікованих даних статистичного дослідження міжбанківської асоціації членів платіжної системи ЄМА (рис. 1.6) в Україні найбільш популярними видами шахрайства через банкомат є кеш-треппінг та скіммінг.

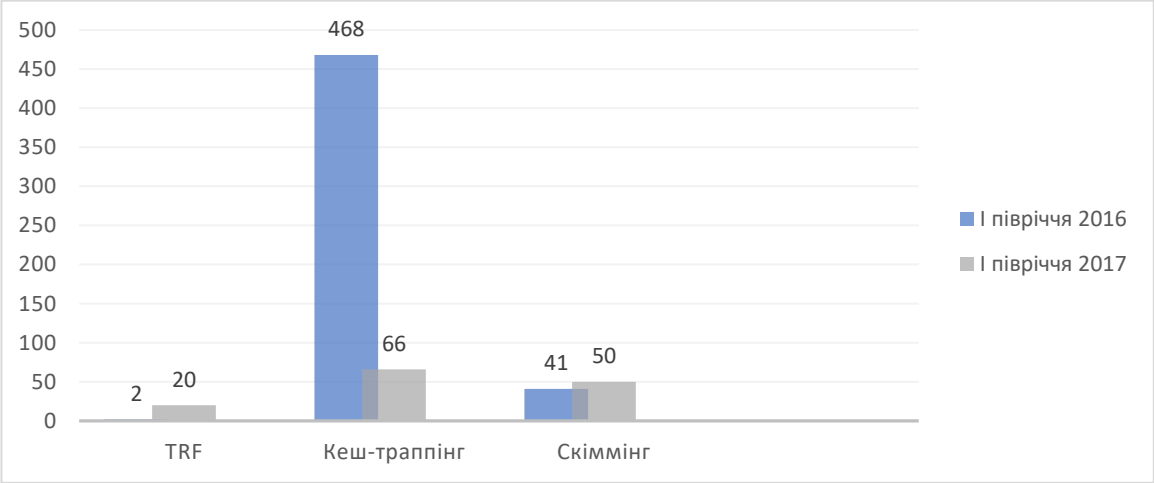

Рис. 1.6. Кількість інцидентів банківського шахрайства [17]

Всі вищеописані види кіберзлочинів спрямовані насамперед на отримання карткових реквізитів для доступу до фінансових ресурсів клієнтів. Ці види шахрайства впливають на фінансовий стан клієнтів банку, а не на сам банк.

Отже, фінансовий сектор економіки, а саме банки та їхні послуги, вважається найпривабливішим для кіберзлочинців, а фінансові дані є одним із найпопулярніших об’єктів кібератак, адже їх використання дає змогу зловмисникам отримувати значні грошові прибутки.

За оцінками Інтерполу, прибутки від скоєння кіберзлочинів у банківській сфері посідають третє місце у світі після доходів від незаконного обігу наркотичних засобів та нелегального постачання зброї [11, с. 81].

Ендрю Хелдейн, керівник відділу фінансової стійкості та стабільності Банку Англії, вважає, що сьогодні найвпливовіші банки Великобританії бояться кіберзлочинів більше, ніж боргової кризи. Але хоча проблема

кіберзлочинності є досить значущою, проте сама система захисту проти кібератак у банківській сфері досі перебуває на початковому етапі розвитку [12, с. 87].

Найбільш поширеними злочинами в банківській сфері є шахрайство з використанням платіжних карток та їхніх реквізитів, несанкціоноване списання коштів із банківських рахунків, утручання в роботу Інтернет-банкінгу, розповсюдження комп'ютерних вірусів, DDoS-атаки на Інтернет-ресурси, шахрайство в інформаційних мережах. Якщо середній показник таких злочинів у країнах Європейського Союзу становить 0,07%, то в Україні кількість подібних злочинів сягає 0,045% усіх операцій із платіжними картками.

Роль НБУ в системі протидії кіберзлочинноті в кредитно-банківській сфері зумовлена його специфічним подвійним правовим статусом. Як орган державного управління він є одним із ключових суб'єктів, які мають забезпечувати функціонування системи кіберзахисту у кредитно-банківській сфері. Водночас, будучи банком, НБУ сам підлягає захисту.

Внутрішніми користувачами (якими є співробітники банків) скоюється близько 60% злочинів, тоді як зовнішніми – тільки 40%. Зазвичай під час «внутрішніх» перевірок порушення порядку здійснення банківських операцій співробітникам служб безпеки банків удається виявити приблизно 10–15% шахрайств, які вчиняються уповноваженими працівниками банків (рис. 1.7) [15].

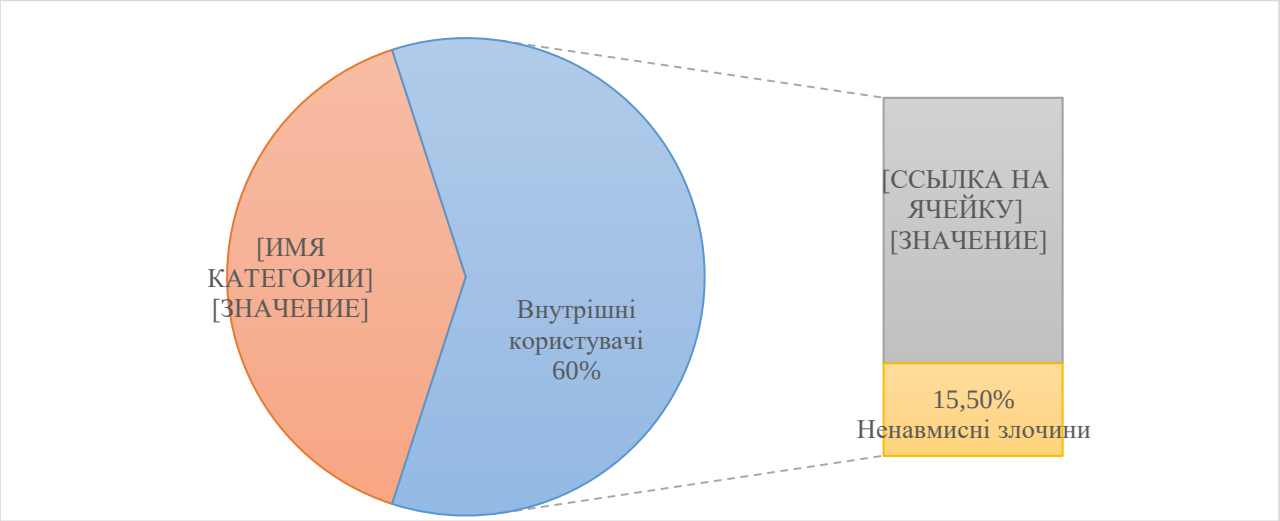

Рис. 1.7. Особи, які несуть відповідальність за кібератаки [11, с.359]

Таким чином, 15,5% кібератак було скоєно ненавмисно, тобто працівники помилково надавали доступ зловмисникам до мережі.Результати виявлення вчинених шахрайств керівники банків також намагаються віднести до банківської таємниці.

У цілому такі наслідки можливо розділити на такі групи: фінансові, іміджеві (репутаційні), юридичні, технологічні (рис. 1.8).

Рис .1.8. Наслідки кіберзлочинів у банківській діяльності [11, 359]

Унаслідок кібератак виникає серйозна загроза належній реалізації основних прав та свобод осіб (клієнтів, засновників банку тощо) у фінансовій сфері життєдіяльності суспільства.

Так, виникає загроза несанкціонованого доступу до приватної, конфіденційної та іншої інформації, її знищення чи пошкодження. Інформатизація діяльності акціонерно-комерційного банку може стати серйозною загрозою для банківської таємниці та прав і свобод фізичних й юридичних осіб.

ВИСОВКИ ДО РОЗДІЛУ 1

1. Актуальною проблемою, з якою зіштовхнулись усі країни у XXI ст. і яка перманентно експоненційно збільшується як за своїми масштабами, так і за рівнем спричиненої шкоди є кіберзлочинність. Незважаючи на комплекс заходів, які вживаються окремими фізичними та юридичними особами, а також державою, кіберзлочинці успішно продовжують свою діяльність у кіберпросторі. У зв'язку із цим нині особливо важливо переглянути усі наявні заходи та активно розробляти нові, що принесуть більшу користь та сформують надійну систему реалізації національних інтересів у кібернетичному просторі через формування надійного механізму профілактики кіберзлочинності.

2. Кіберзлочинність – це сукупність суспільно небезпечних діянь, що вчиняються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, компютерних мереж і комп'ютерних даних. Дане визначення охоплює всі види злочинів в ІТ-сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть стати предметом, засобом або знаряддям злочинних посягань, а також середовищем, в якому відбуваються правопорушення.

3. Наслідки кіберзлочинності зачіпають не лише інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство загалом. Кіберзлочини найчастіше ставлять під загрозу життєво важливу як інформаційну, так і взагалі критичну інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства. Таким чином можна стверджувати, що кіберзлочинність виступає загрозою національній безпеці в кібернетичній сфері.

4. Тенденції розвитку суспільних відносин в Україні протягом останніх років демонструють такі найбільш поширені кіберзлочини: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем із метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини.

5. Пріоритетними напрямами забезпечення кібербезпеки банківської системи України є:

—моніторинг кіберпростору для своєчасного запобігання кіберзагрозам;

—захист інформаційних ресурсів банку з урахуванням практики розвинених країн світу;

—створення системи підготовки кадрів у сфері кібербезпеки в банках;

—розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки.

РОЗІДЛ 2
АНАЛІЗ ДІЮЧОЇ ПРАКТИКИ БОРОТЬБИ З КІБЕРЗЛОЧИНАМИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

2.1. Нормативно-правове й інституційно-організаційне забезпечення протидії кіберзлочиннам в банківській сфері

Сучасний стан розвитку інституту міжнародно-правової протидії кіберзлочинності характеризується регіональним характером та інтенсифікацією уніфікації національних законодавств. За умов відсутності єдиного універсального міжнародного договору про кіберзлочинність, основні конвенційні засади містяться в положеннях чинних регіональних угод:

1) Конвенція про кіберзлочинність Ради Європи, прийнята 21.11.2001 року та Додатковий протокол від 28.01.2003 р. (далі – Будапештська конвенція) [52];

2) Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. (далі – Конвенція ЛАД) [59];

3) Угода про співробітництво держав – членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01.06.2001 р. (далі – Угода СНД) [12]. Нова редакція цієї Угоди була відкрита для підписання у 2018 р., однак поки ще не вступила в силу;

4) Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (далі – Угода ШОС);

5) Конвенція про кібербезпеку і захист персональних даних Африканського Союзу від 27.06.2014 р. (далі – Конвенція АС).

Фактично, в текстах усіх зазначених актів містяться види протиправних діянь, що підлягають криміналізації в національних правових системах держав-учасниць. Варто відзначити, що важливим питанням є співвідношення сфер дії цих договорів та їх узгодження. Зокрема, враховуючи той факт, що Конвенція про кіберзлочинність Ради Європи отримала поширення за рамки європейського регіону (ратифікована 18 державами та підписана 25 країнами, серед яких Україна), застосування перелічених міжнародно-правових актів може відбуватись паралельно.

Перші кроки щодо протидії кіберзлочинам в Україні були здійснені у 1994 році, коли до Кримінального кодексу 1960 року було внесено зміни, якими в ст. 198-1 «Порушення роботи автоматизованих систем» передбачено кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи носіїв інформації. Однак у 2001 році був прийнятий Кримінальний кодекс України (КК України), відповідно до якого ця діяльність вийшла на якісно новий рівень. Так, у вказаному нормативно- правовому акті діянням у сфері інформаційної безпеки було присвячено окремий розділ – XVI «Злочини у сфері

використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [59, с.115].

Загалом, розвиток інформаційних технологій супроводжується значною криміналізацією економічної сфери. Звісно, держава не залишає без уваги питання боротьби з такими злочинами, намагаючись постійно вдосконалювати законодавство, що регулює відносини в зазначеній сфері. Законом України від 5 червня 2003 року № 908-IV були внесені зміни до вказаного Кодексу, відповідно до яких розділ VI Особливої частини Кримінального кодексу України «Господарські злочини» зазнавав чи не найбільших змін порівняно з іншими розділами. Це було викликано підвищенням суспільної небезпеки, кількісним зростанням відповідних посягань, а також тим, що значна частина економіки України працює в «тіні». Також треба зазначити, що на даному етапі розвитку суспільства саме банківська система держави, яка пов'язана з накопиченням, розподілом і використанням державних і приватних коштів, є однією з найбільш привабливих для окремих злочинців і, особливо, організованих злочинних груп. Злочини, що вчиняються у банківській системі або з її використанням, можна віднести до одних із найбільш небезпечних економічних посягань, оскільки їх негативний вплив відображається не тільки на самому банку, але й на багатьох інших суб'єктах економічної діяльності і фінансовій системі держави в цілому, адже часто одержані злочинцями кошти переводяться за межі України, що призводить до прискорення інфляційних процесів, знецінення національної валюти та інших негативних наслідків для кредитно-фінансової системи.

Особливо великих розмірів досягають суми, які знімаються з банківських рахунків, як вкладників, так і ресурсів самих банків, з використанням комп'ютерних систем. Тому, говорячи про злочини у банківській сфері, не можна оминути увагою так звані кіберзлочини – передбачені кримінальним законом суспільно небезпечні діяння, для скоєння та розслідування яких застосовуються комп'ютерні технології та/або використовується глобальна

мережа Інтернет. Очевидно, що ця група злочинів досить широка і включає діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. Дана група злочинів також має високий рівень суспільної небезпеки, адже характеризується високим рівнем професійної злочинності, значним відсотком злочинності високоосвічених суб'єктів; високим ступенем ураженості економічної і господарської сфери внаслідок вчинення даного злочину, та має транснаціональний, міжнародний характер, що властивий для найбільш небезпечних різновидів аналізованої злочинності.

Отже, можна помітити, що у перерахованих вище сферах (а саме, господарська діяльність та кіберзлочинність) виділяється певна група суміжних злочинів, до яких зокрема відноситься і злочин, передбачений статтею 200 Кримінального кодексу України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення».

Злочинна діяльність такого спрямування характеризується різноманітністю, високоінтелектуальним характером, швидкою адаптацією нових технологій для вчинення протиправних дій, що дозволяє відносити дані злочини до категорії особливо складних та вимагає застосування додаткових знань та можливостей. Розслідування таких діянь у багатьох випадках надто ускладнюється тим, що наразі у правоохоронних органах недостатньо кваліфікованих спеціалістів, тобто такі злочини залишаються досить складними для слідчого пізнання, та методика їх розслідування досі ще недостатньо розроблена.

Боротьба зі злочинністю неможлива без використання системи правових заходів. Важливе значення має наявність спеціальних законів у сфері вчинення злочину, які регулюють певні суспільні відносини. В даному випадку таке законодавство наявне, це зокрема Закон України «Про платіжні системи та переказ грошей в Україні» та Закон України «Про банки і банківську діяльність». Загалом, діяльність автоматизованої банківської системи (АБС) забезпечується і регулюється на основі законодавчих актів і

рекомендацій Національного банку України, основні нормативні акти якого представлені на рис. 2.1.

Проведений аналіз законодавчої бази України показав, що для забезпечення захисту інформації в АБС використовуються системи управління інформаційною безпекою (СУІБ), що забезпечують контроль функціонування комплексних систем захисту інформації

Але основну роль серед правових засобів боротьби відіграє визначення даного діяння як злочину та встановлення кримінально-правової відповідальності за його вчинення у Кримінальному кодексі України.

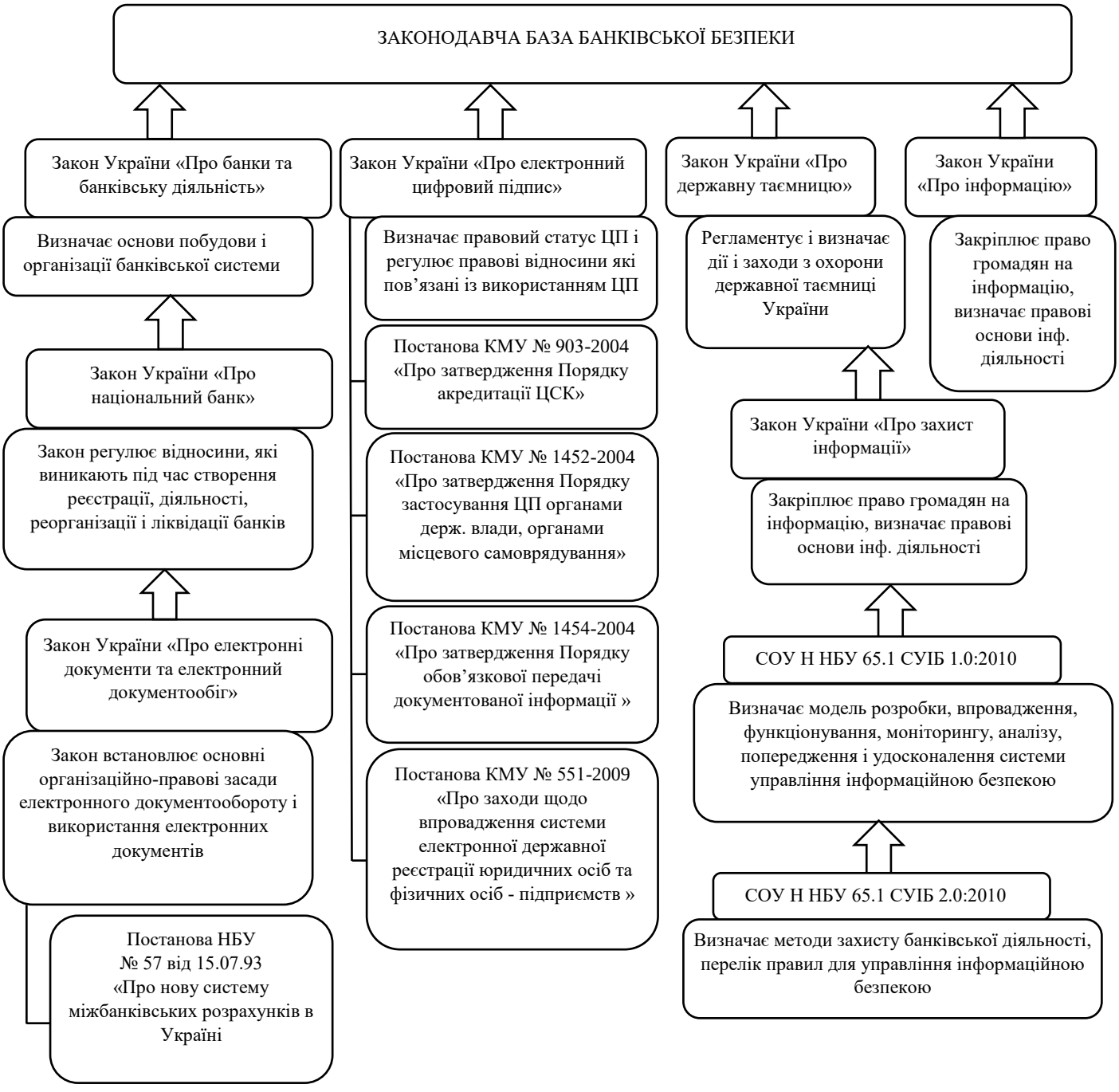

Рис. 2.1. Нормативна база діяльності автоматизованих банківських систем

Аналізуючи склад злочину, передбаченого ст. 200 Кримінального кодексу, треба звернути увагу, що обов'язковим елементом об'єктивної сторони даного діяння є предмет. Предметом злочину, передбаченого ст. 200 КК України, є будь-які засоби доступу до банківських рахунків при вчиненні злочину у формі їх підробки; підроблені документи на переказ чи підроблені платіжні картки при вчиненні злочину у формі їх придбання, зберігання, перевезення чи пересилання з метою збуту, а також їх використання чи збуту.

Безпосередньо у диспозиції ч. 1 ст. 200 КК названі два види засобів доступу до банківських рахунків – документи на переказ та платіжні картки. У назві ст. 200 називається ще один предмет злочину – обладнання для виготовлення засобів доступу до банківських рахунків, тобто коло предметів злочину у ній описується більш широко [3].

Враховуючи правила тлумачення кримінально-правових норм, обладнання для виготовлення засобів доступу до банківських рахунків не є предметом передбаченого ст. 200 Кримінального кодексу злочину. А оскільки обладнання для виготовлення засобів доступу до банківських рахунків – це комплексна категорія, яка має відображати виготовлення документів на переказ (як в паперовому, так й електронному виді), платіжних карток та інших засобів доступу до банківських рахунків, та яка характеризується наявністю апаратних та програмних засобів, то вважається за доречне доповнити диспозицію аналізованої норми та передбачити, що об'єктивна сторона даного злочину повинна включати й незаконні дії щодо обладнання для виготовлення засобів доступу до банківських рахунків.

Продовжуючи аналізувати зміст диспозиції ч. 1 ст. 200 Кримінального кодексу, також треба звернути увагу на передбачену у статті мету злочинних дій, а саме це мета збуту [3]. Вважається, що ефективним може бути розширення положення щодо мети зазначеного діяння, та доповнення його метою використання. Це буде більш логічно та дозволить охопити

кримінальною відповідальністю більш широке коло злочинних дій, адже особа-злочинець може придбавати, зберігати, перевозити або пересилати підроблені документи на переказ чи платіжні картки з метою особистого використання, а не збуту, але саме використання ще не здійснити. Такі дії вже можна вважати суспільно-небезпечними, адже мета цих дій – порушення належного функціонування банківської системи.

Таким чином, диспозицію ч. 1 ст. 200 Кримінального кодексу треба викласти в такій редакції: «Підробка документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання, перевезення, пересилання з метою збуту та/або використання підроблених документів на переказ платіжних карток чи обладнання для їх виготовлення, або їх використання чи збут…».

Оскільки злочин, передбачений ст. 200 Кримінального кодексу, є злочином з формальним складом, то відповідальності за наслідки зазначених діянь не встановлено. Можна не погодитись з законодавцем щодо цього, адже не доречно передбачати однакову відповідальність за діяння, якщо воно взагалі не спричинило ніяких наслідків, та за те ж саме діяння, якщо воно нанесло значної шкоди потерпілим, як це вочевидь може статися при вчиненні аналізованих дій. Тому наголошується, що структурно ст. 200 треба доповнити частинами, які будуть передбачати відповідальність за ті самі дії, якщо вони спричинили збитки у великих чи особливо великих розмірах.

Кримінальна відповідальність за кіберзлочини передбачена різними розділами та статтями КК України. Це розділ XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електронного зв’язку» (ст. ст. 361, 361-1, 361-2, 362, 363, 363-1); ч. 3ст. 190 «Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки»; ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення».

Досліджуючи правові заходи боротьби зі злочином, передбаченим ст. 200 Кримінального кодексу, не можна оминути увагою значення такого заходу, як відповідальність, що встановлена санкцією ст. 200 КК України – покарання у вигляді штрафу від 3 до 5 тисяч неоподатковуваних мінімумів доходів громадян. А у кваліфікованому складі передбачене покарання у вигляді штрафу від п’яти до десяти тисяч неоподатковуваних мінімумів доходів громадян [3].

До внесення змін Законом України «Про внесення змін до деяких законодавчих актів України щодо гуманізації відповідальності за правопорушення у сфері господарської діяльності» [4] у Кримінальний кодекс санкція ст. 200 передбачала покарання у вигляді штрафу від 500 до 1000 неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років, або позбавлення волі на той самий строк. А у кваліфікованому складі було передбачене покарання у вигляді позбавлення волі на строк від двох до п’яти років. Тобто, має місце підвищення міри майнового покарання (збільшення розміру штрафів), що є доречним для даної статті, але при цьому і певна гуманізація покарання в цілому. Але, як вже зазначалося, злочинна діяльність, передбачена ст. 200 Кримінального кодексу, охоплює важливі сфери суспільного життя та наносить збитків економічній системі держави. Тому можна констатувати, що внесені зміни не є цілком виправданими та доречними.

Більш ефективно боротьбі зі злочином, передбаченим ст. 200 Кримінального кодексу, сприяло б встановлення штрафу, як додаткового виду покарання у поєднанні з обмеженням чи позбавленням волі у якості основного покарання, адже даний злочин скоюється тільки з метою отримання майнової вигоди та наносить майнову шкоду потерпілим від злочину. Таким чином, якщо взяти за основу санкцію, яка існувала до внесення змін у ст. 200 Кримінального кодексу, можна передбачати два види покарання: обмеження волі на строк до трьох років та штраф від 500 до 1000 неоподатковуваних мінімумів доходів громадян або позбавлення волі на той

самий строк та штраф від 500 до 1000 неоподатковуваних мінімумів доходів. Звичайно, можна змінити розмір штрафу, виходячи з економічної ситуації в країні. За ч. 2 ст. 200 Кримінального кодексу також повинно передбачатись поєднання позбавлення волі та штрафу.

Щодо відповідальності за злочинні дії, передбачені ст. 200 Кримінального кодексу, якщо вони спричинили збитки у великих чи особливо великих розмірах, то доречно буде, окрім основного покарання, застосовувати такий вид додаткового покарання, як конфіскація коштів або іншого майна, отриманого злочинним шляхом. Тобто, санкції зазначених частин повинні передбачати покарання у вигляді позбавленням волі на певний строк з конфіскацією коштів або іншого майна, отриманого злочинним шляхом.

Таким чином, проаналізувавши зміст та структуру ст. 200 Кримінального кодексу України можна звернути увагу на значну кількість недоліків у юридичній техніці, а також вади загальної побудови статті та недосконаліть видів та міри юридичної відповідальності, які встановлено в санкції. Саме тому можна зробити висновок, що внесення відповідних змін до ст. 200 КК України буде важливим для попередження вчинення злочинів даної категорії, дозволить охопити відповідальністю більш широке коло протиправних діянь, які порушують нормальне функціонування банківської системи України, та сприятиме реалізації принципів повноти та справедливості покарання, а отже зробить правові засоби боротьби з даними злочинами більш ефективними.

Дані огляду в сфері інформаційної безпеки свідчать про те, що кіберзлочини стають більш витонченими, що ускладнює їхнє виявлення та запобігання. Це може призвести до ще більших збитків і втрат у майбутньому.

Ураховуючи транскордонний характер кіберзлочинності, потребує налагодження співробітництво правоохоронних органів у розслідуванні кіберзлочинів на оперативному рівні; створення і забезпечення

функціонування механізму вирішення юрисдикційних питань у кіберпросторі. У сучасному інформаційному суспільстві, де поширені і будуть надалі поширюватись кіберзагрози, важливо постійно і системно, своєчасно вживати ефективних заходів із протидії кіберзлочинності, а також удосконалення її методів і форм її попередження. Це стосується практично всіх сфер суспільного і державного життя, підприємницького і соціогуманітарного середовища. З огляду на курс України на входження у світовий інформаційний простір ми переконані, що потребує побудови національна модель забезпечення кібербезпеки підприємств, установ і організацій, включаючи неурядових; координація зусиль та взаємодія правоохоронних органів, спецслужб, судової системи, а також належне їх кадрове і матеріально-технічне забезпечення, обмін інформацією про попередження і боротьбу з кіберзлочинністю.

2.2. Аналітична характеристика кіберзлочинності у банківській сфері

Банківська система є однією з головних ланок фінансово-кредитної системи країни. За часту вона є одним з об’єктів, які приваблюють шахраїв та злочинців, що підриває авторитет банків, як гарантів збереження та накопичення коштів населення, держави та суб’єктів господарювання.

Щоб зрозуміти масштаб загрози, можна звернутися до даних дослідження, які в 2018 році опублікував Майкл МакГуайр, викладач кримінології в Університеті Суррея в Англії. Так, за його підрахунками, загальний обсяг доходів кіберзлочинців в 2018 році склав 1,5 трильйона доларів, що є величезним числом (рис. 2.2).

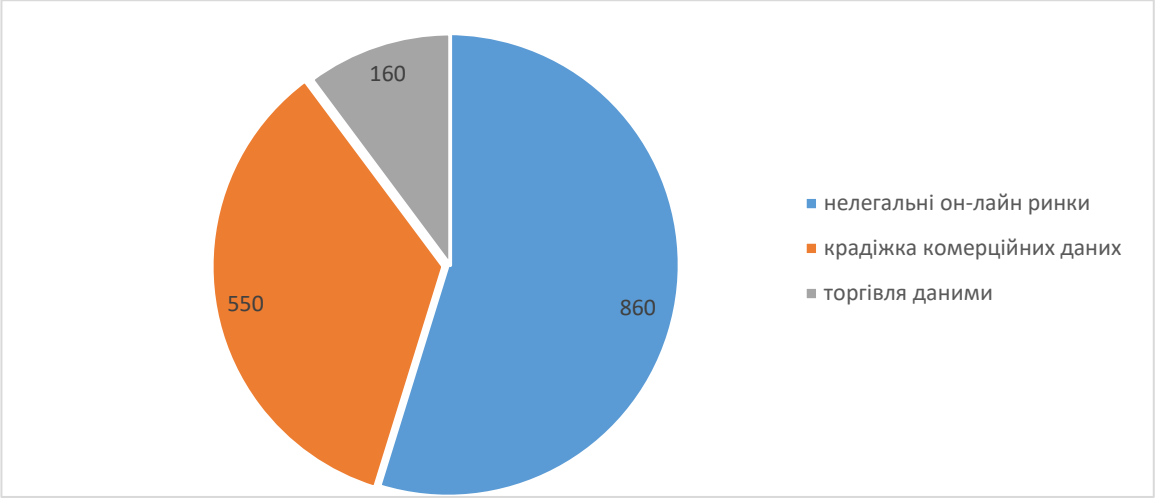

Рис. 2.2. Доходи кіберзлочинців в 2018 році, в цілому по світу [30, с.1013]

Основна маса доходів злочинців йде з нелегальних онлайн-ринків, які не мають ніякої реєстрації і не звітують про свої транзакції, і як мінімум не платять податки. Все це породжує нечесну конкуренцію, яка приносить збитки законослухняним організаціям на фінансовому ринку. Нелегальні фінансові ринки не контролюються державою, тобто немає гарантії безпечної участі на них, а учасники даних ринків не платять податки, що позбавляє бюджет частини коштів, які повинні бути сплачені згідно законодавства.

Найбільший обсяг розкрадань доводиться на США і країни ЄС, так як вони мають найбільшу фінансову та інвестиційну привабливість. На сьогодні, найбільша кількість злочинів спостерігається у фінансовій сфері. З метою крадіжки грошових коштів створюються хакерські групи такі як Cobalt, MoneyTaker, Lazarus, частина з яких є російськомовними [30]. Наведені угруповання є найбільш небезпечними для банків на міжнародній арені, оскільки їм не складає великих труднощів атакувати і вивести з ладу банк, а пізніше вилучити грошові активи. У 2018-му році було виявлено нове хакерське угруповання – Silence, яке отримало назву «нової загрози для банків» [30].

Згідно з даними Американської асоціації банкірів, у світі здійснюється понад 2,5 трлн. операцій за кредитними картками у рік. Картки приймаються у понад 24 млн. точках у понад 200 країнах. Щосекунди здійснюється

приблизно 10 тис. операцій за допомогою банківських карток [1]. Саме тому у багатьох країнах світу кіберзлочинність у банківській системі є небезпекою номер один. І як результат, ідентифікація та оцінка ризику шахрайства в умовах функціонування електронного банкінгу є одним із пріоритетних завдань для банківських установ, які використовують інформаційні технології у процесі банківського обслуговування.

Проблематикою кіберзлочинів у банківській сфері займаються останні 10-15 років, що пов'язано із зростанням науково-технічного прогресу в галузі інформаційних технологій та програмного забезпечення, а також із збільшенням доступності до інформації з боку звичайного користувача. Однак, з кожним роком способи шахрайств модифікуються, відповідно банківські служби кібербезпеки не встигають удосконалювати методи боротьби з ними.

На сьогодні питання боротьби з кібершахрайством є актуальним і для України, оскільки дана проблема торкається різних суб'єктів – держави, банків, суб'єктів господарювання та населення. Не дивлячись на проведення різних активних заходів, робота в цьому напрямку не є системною. Кожний банк впроваджує свої заходи та програмне забезпечення, які за часту не є ефективними; НБУ здійснює тільки регламентацію положень та формує рекомендації щодо створення системи захисту.

В результаті населення стає все частіше об'єктом шахрайств, втрачає довіру до банків, як фінансових інститутів, що призводить до втрати банками клієнтів.

В Україні за 2017 рік кібершахраями було вкрадено 670 млн грн., при тому що у 2016 році майже удвічі менше – 339 млн грн. Це свідчить про те, що заходи кібербезпеки, організовані у банках, не є досить ефективними. Хоча дану проблему широко популяризують через засоби масової інформації, проводиться роз'яснювальна робота з даного питання серед населення, але випадки шахрайств все одно зростають. Як уже зазначалось,

методи шахраїв модифікуються, що потребує також модифікації системи захисту в банках.

Впровадження банківських карт і використання комп'ютерних технологій в сфері платежів є характерною рисою повсякденного життя. Швидкими темпами розвиваються безготівкові форми розрахунків. Платежі, що здійснюються без участі готівки, сприяють прискоренню оборотності, скороченню кількості грошових коштів, необхідних в обігу, що, як наслідок, призводить до зниження витрат обігу, збільшенню прозорості розрахунків [1]. Завдяки своїй простоті, масовості, доступності технологій, операції з банківськими картками найбільш приваблюють шахраїв.

З 01.01.2017 року по 26.08.2017 рік платіжні сервіси системи Exchange-Online зафіксували 12416 підозрілих операцій на загальну суму 3409000 гривень. В операціях прийняло участь 7390 банківських карт 135 банків з 53 країн, в тому числі з 67 українських банків. Дані кошти кіберзлочинці намагалися вивести за допомогою мобільних пристроїв [2].

На рис. 2.3 представлено країни, за карками яких проводились спроби операцій, ідентифікованих системою, як кіберзлочини, та відсоток операцій, які дійсно виявилися шахрайськими.

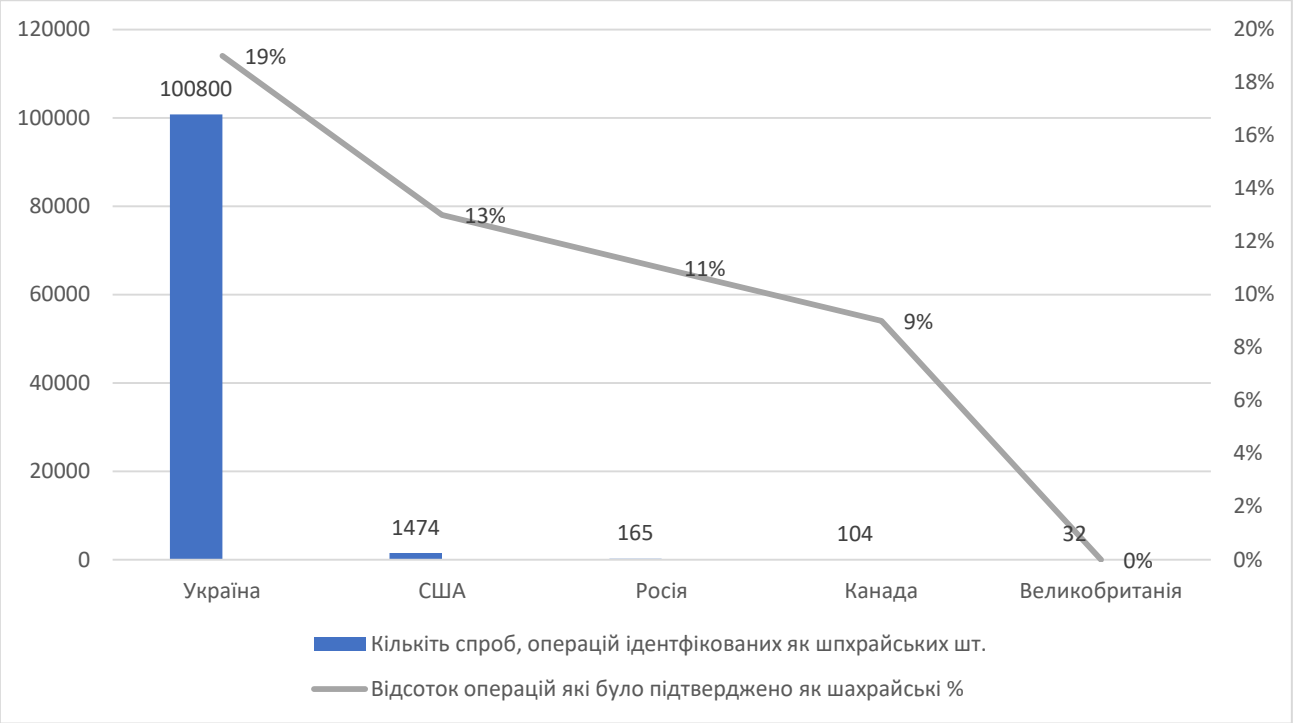

Рис. 2.3. Аналіз шахрайських операцій, здійснених у 2018 році [109, с.838]

Дані рисунку свідчать про те, що Україна займає лідуюче місце та втрапила в п'ятірку країн, в яких банківські платіжні операції є не досить захищеними. Виявилося, що 19 % операцій є дійсно шахрайськими і це перевищує обсяги шахрайств в інших країнах. З допомогою кібершахрайств з карток українців було знято 238955 гривень. Тобто, банківські платіжні системи через слабкий захист потенційно можуть втрачати клієнтів через той факт, що вони можуть стати об'єктами шахрайства. Тому це не тільки проблема банків, але й соціальна проблема, яку потрібно вирішувати комплексно та із залученням різних структур – держави, населення, банків, інвесторів.

За останні декілька років в Україні різко збільшилася кількість безготівкових транзакцій: поповнення мобільних, переказ між рахунками, покупки в інтернеті. А в минулому році наша країна стала четвертою в світі за кількістю безконтактних платежів. І це величезне поле можливостей для кіберзлочинів. На рис. 2.4 наведені групи шахрайських операцій,

здійснених протягом 2017–2018 років та об'єднаних за однаковим способом здійснення, які представлені у відсотках.

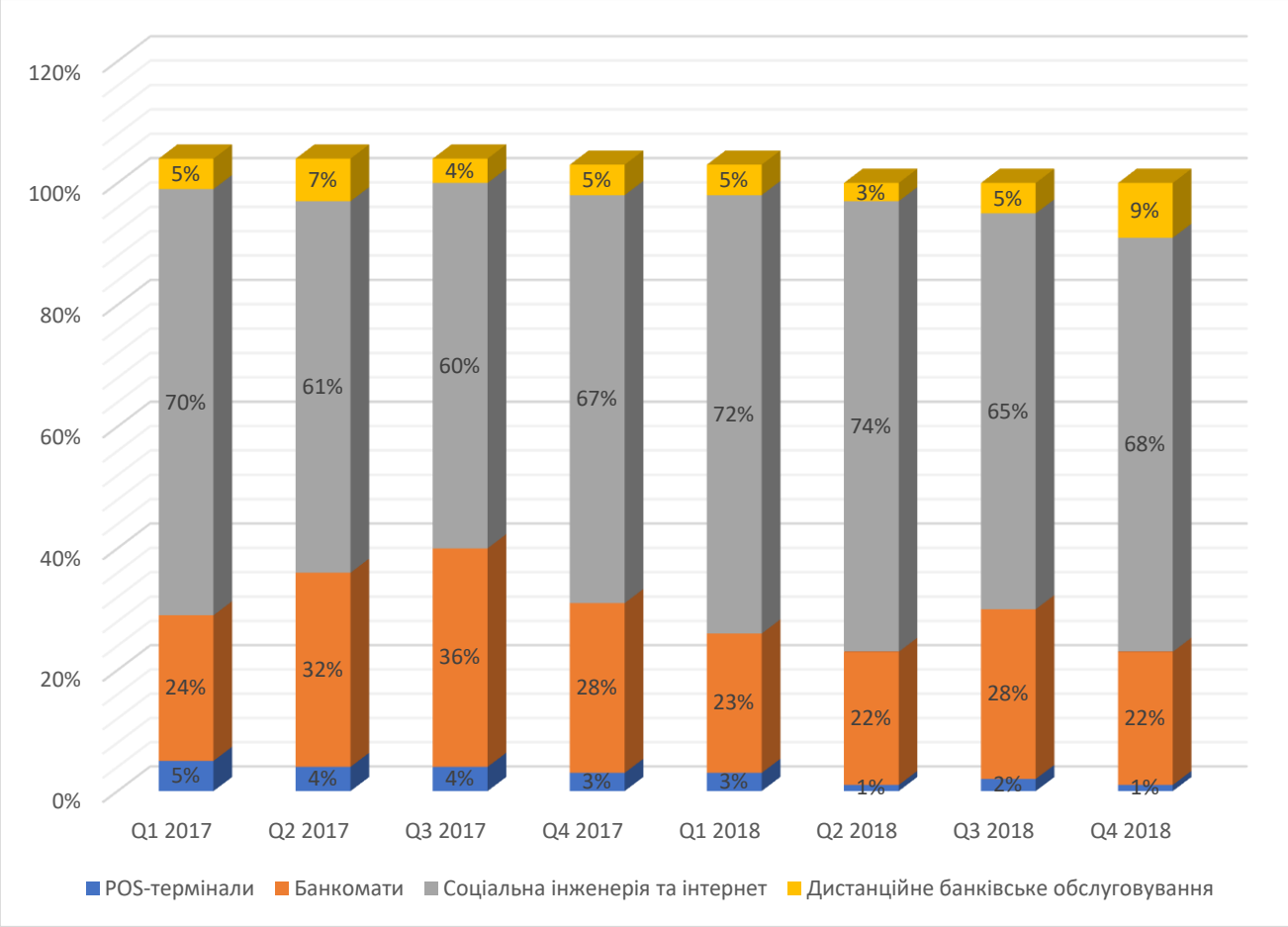

Рис. 2.4. Тенденції розвитку кіберзлочинів за видами [17]

Найбільша доля шахрайських операцій, які було здійснено за допомогою методів соціальної інженерії (60–74%), включають в себе здійснення вішингу та фішингу, тобто кіберзлочинці виманюють дані платіжних карток у клієнтів, отримують доступ до рахунків та знімають кошти. Зазвичай жертвами соціальної інженерії стають літні люди (від 55 і старші) – 15%, і середнього віку (35–44) – 13%.

Ще декілька років тому кіберзлочинці масово використовували технологію кеш-треппінг (Cash Trapping). У 2015-2016 роках спостерігалася найбільша кількість таких злочинів, а саме 991 та 817 відповідно. Масштабна інформаційна кампанія сприяла зменшенню випадків кеш-треппінгу до 90 у 2018 році (рис. 2.5).

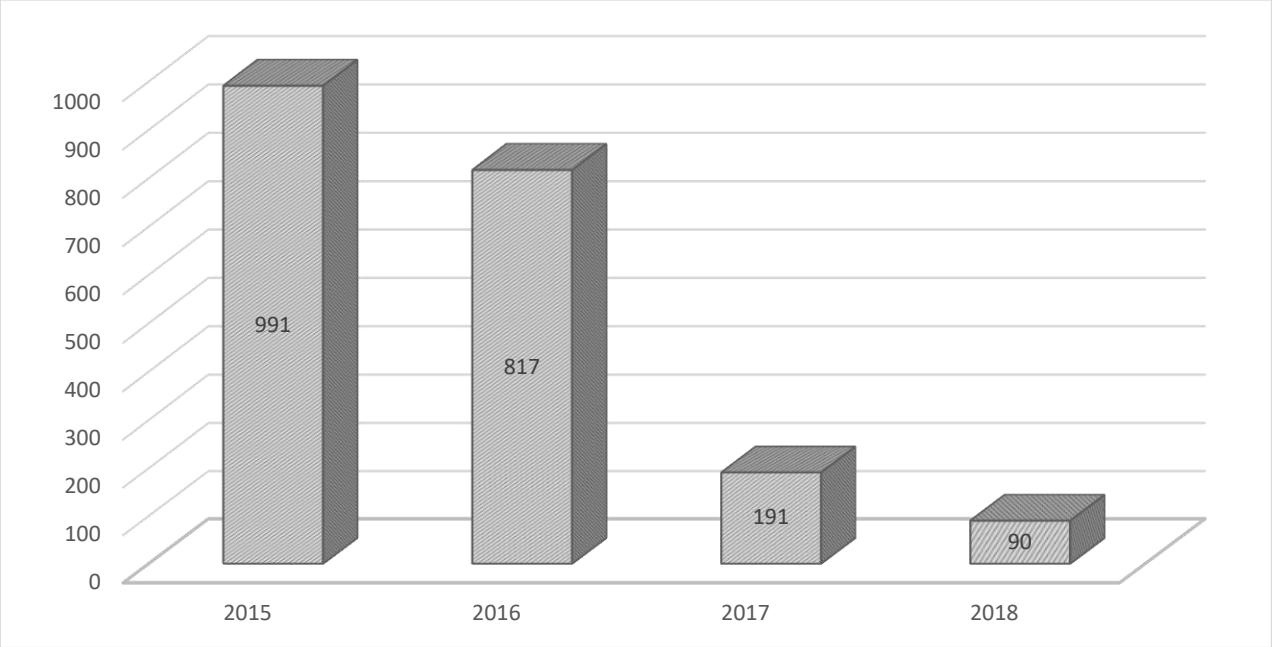

Рис. 2.5. Кількість випадків кеш-треппінга [17]

Ще одним популярним видом банкоматного шахрайства став скіммінг (skimming), суть якого полягала у копіюванні даних магнітної смуги банківської карти за допомогою спеціального пристрою, який злочинці встановлювали у картрідер банкомату. За допомогою цієї інформації злочинці виготовляли дублікат карти і потім знімали готівкові кошти. Оскільки банки стали випускати більше чіпових карт, частота даного виду злочину дещо знизилася, однак залишається ще досить високою (рис. 2.6).

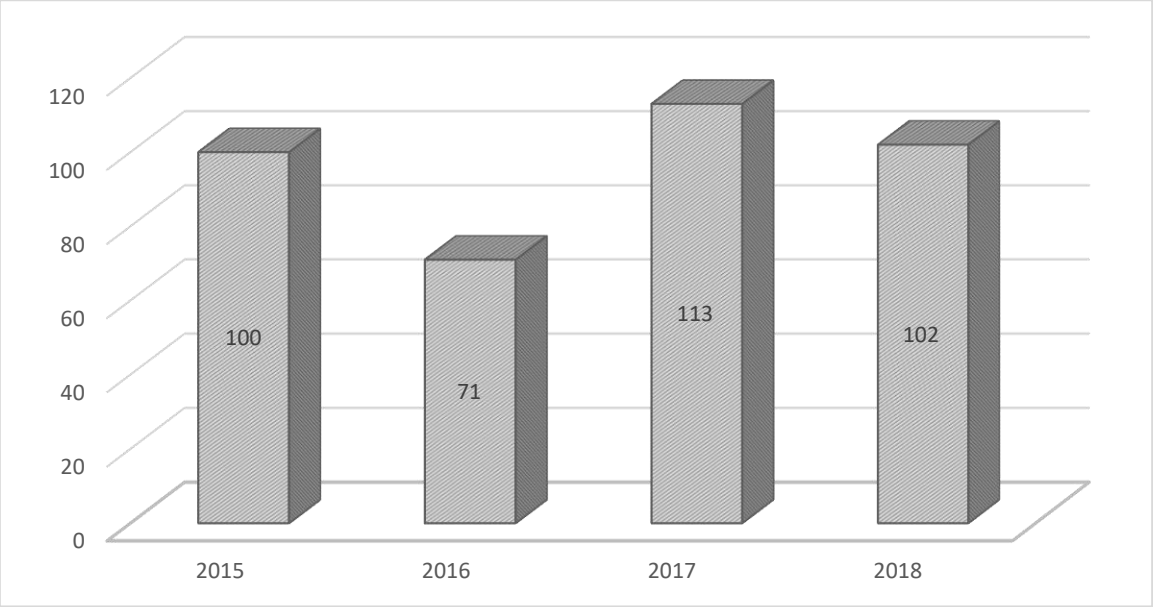

Рис. 2.6. Кількість випадків скіммінгу

Кіберзлочини здійсненні шляхом соціальної інженерії – це глобальна проблема. Станом на кінець першого кварталу 2017 року найбільшої шкоди від фішингових атак зазнали 51,70% банків світу. До країн з найвищим відсотком нападу на користувачів відносяться: Китай (20,87%), Бразилія (19,16%), Макао (11,94%), Російська Федерація (11,29%), Австралія (10,73%), Аргентина (10,42%), Нова Зеландія (10,18%), Катар (9,87%), Казахстан (9,61%), Тайвань (9,27%) [16, с.334].

За часткою атакованих користувачів від вішингу до найбільш атакованих країн відносяться: Росія (1,2%), Узбекистан (0,40%), Казахстан (0,36%), Таджикистан (0,35%), Туреччина (0,34%), Молдова (0,31%), Україна (0,29%), Киргизстан (0,27%), Білорусь (0,26%) та Латвія (0,23%) [16, с.335].

Досить популярними у кіберзлочинців є способи крадіжок коштів через банкомат (32%) та через Інтернет (16%). Тобто, банківська система кібербезпеки повинна розробити додаткові способи захисту операцій від цих видів кіберзлочинів.

В Україні у 2017 року збитки клієнтів банків від соціальної інженерії склали 509,72 млн грн., що практично вдвічі перевищило збитки за 2016 рік

та у 9 разів за 2015 рік. Протягом 2018 р. спостерігалася позитивна тенденція до зменшення суми збитків до 245,81 млн. грн або майже у 3 рази, що повязано із розяснювальною роботою банківських установ (рис. 2.7)

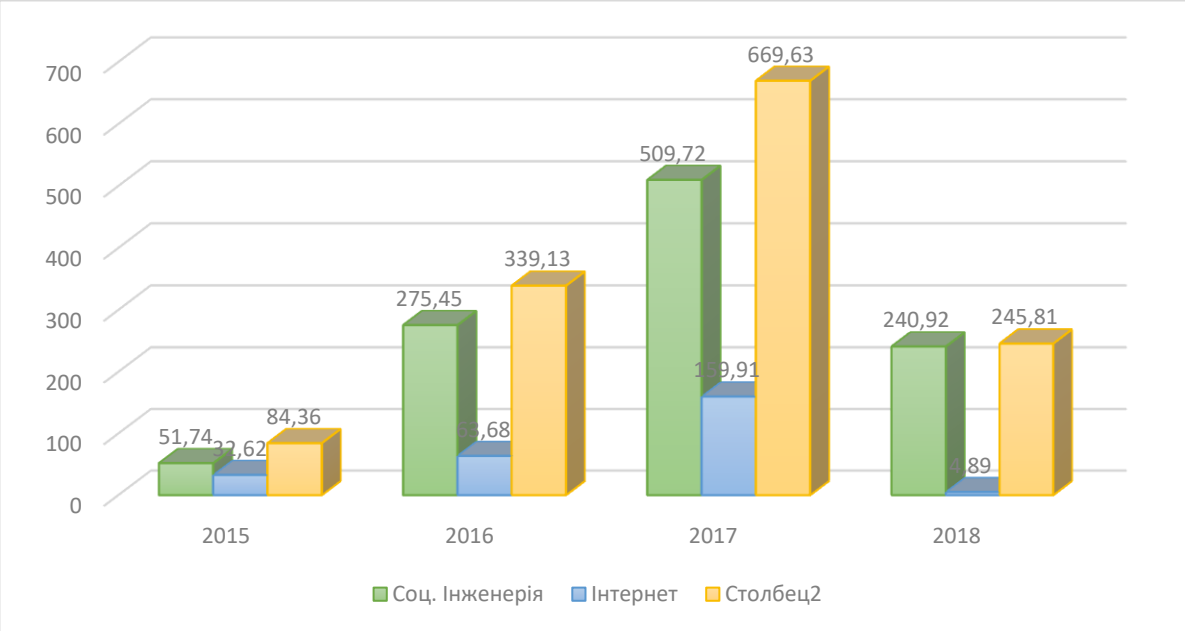

Рис. 2.7. Сукупний розрахунковий дохід кіберзлочинів, млн грн.

Також збільшилася середня сума шахрайської операції, здійсненої за допомогою методів соціальної інженерії, до 2543 грн. у 2017 році, що в 1,8 разів перевищує даний показник у 2016 році та станом на кінець 2018 р. становив 3620 грн. (рис. 2.8).

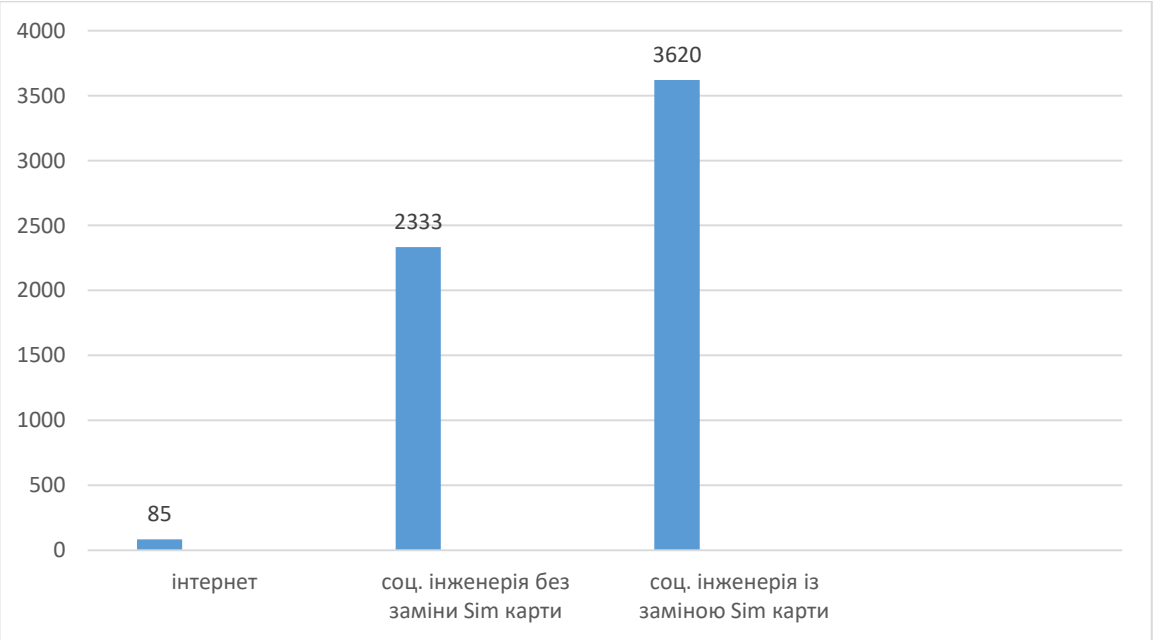

Рис. 2.8. Середня сума шахрайської операції у 2018 році, грн.

Якщо розглядати середню суму шахрайської операції, то методи соціальної інженерії із заміною SIM-карти приносять аферистам набагато більший дохід. Щоб зменшити ймовірність злому, в Приватбанку радять завести окремий, захищений 8-значним пін-кодом фінансовий номер.

Допоможе зменшити кількість подібних злочинів тісніша співпраця банків та мобільних компаній.

У більшості випадків уберегтися від шахраїв допомагає уважність, та моніторинг інформації через Google. Наприклад, номер підозрілого телефону можна перевірити на сайті Чертофон — це чорний список телефонів шахраїв, який оновлюється щодня. У 2018 році база налічувала вже 5 139 телефонів та 2 288 ІПН.

В Україні найбільша кількість випадків платіжних кіберзлочинів з використанням методів соціальної інженерії здійснюється в середовищі Card-Not-Present (операції здійснюються без наявності картки та фізичної присутності користувача), у порівнянні із обслуговуванням через банкомати, POS- термінали та дистанційне банківське обслуговування (рис. 2.9).

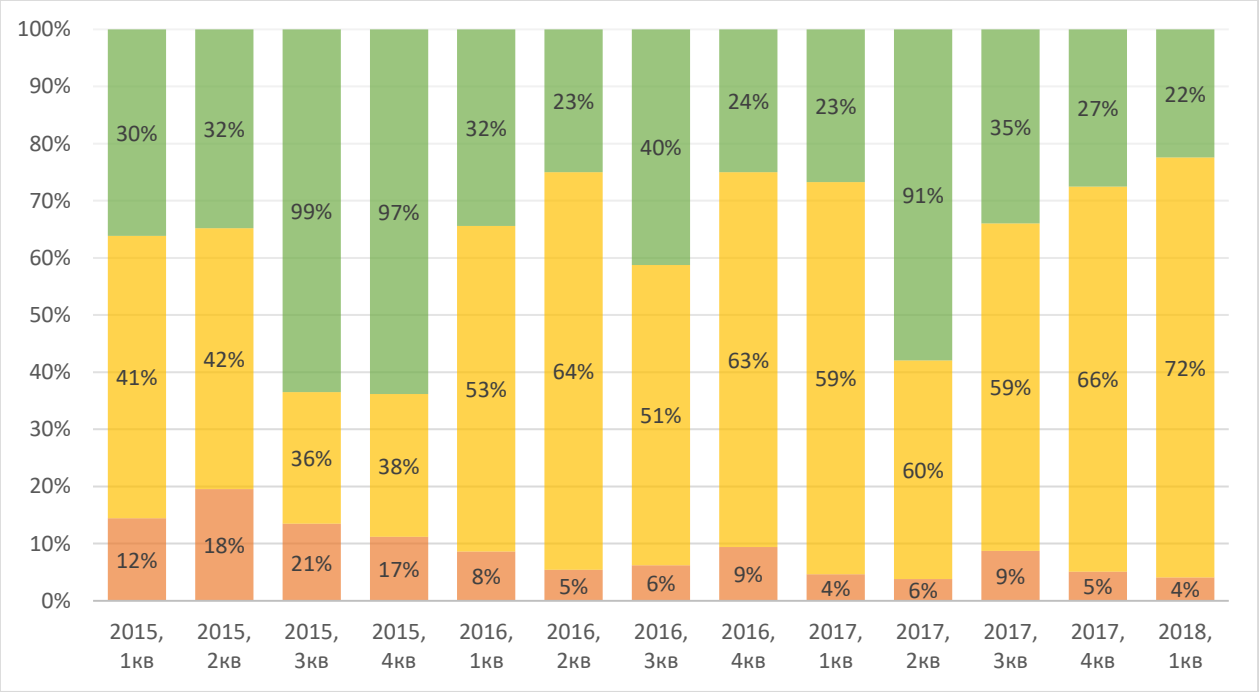

Рис. 2.9. Шахрайські операції за різними видами банківського обслуговування [17]

Методи соціальної інженерії набирають популярності у кіберзлочинців, оскільки зловмисники не тільки отримують дані платіжної картки, але й ідентифікаційні дані клієнта. Також даний спосіб шахрайства є досить простим у здійсненні. Хоча банківські співробітники й попереджають своїх клієнтів не розголошувати платіжну інформацію через телефон, але шахраї мають досить багато способів психологічного впливу на жертву.

На основі проведеного аналізу наслідків кіберзлочинів, які відбуваються в сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об’єктом злочину.

Для боротьби з даним способом шахрайства українські банки не мають досить дієвих інструментів. На нашу думку, для даних видів кіберзлочинів доцільно застосовувати сукупність засобів, що базуються на методах інтелектуального аналізу та інформаційних технологій.

2.3. Напрями протидії інформаційним злочинам у банківській сфері

Революційні зміни останнього десятиліття в електронній промисловості, об’єднання інфокомунікаційних та комп’ютерних мереж в єдиний простір істотно розширили спектр послуг автоматизованих банківських систем (АБС), при цьому фінансово-банківська системи опинилася під загрозою з боку кібератак. Таким чином, вирішення питань забезпечення безпеки транзакцій в АБС залишається актуальною і на сьогоднішній день.

Комп’ютерні системи та телекомунікації забезпечують надійність функціонування величезної кількості інформаційних систем самого різного призначення. Більшість таких систем несуть в собі інформацію, що має конфіденційний характер. Таким чином, рішення задачі автоматизації процесів обробки даних спричинило за собою нову проблему - проблему

інформаційної безпеки [19, с.120]. З часу своєї появи банки незмінно викликали злочинний інтерес. І цей інтерес був пов'язаний не тільки зі зберіганням в кредитних організаціях грошових коштів, але і з тим, що в банках зосереджувалася важлива і часто секретна інформація про фінансової та господарської діяльності багатьох людей, компаній, організацій і навіть цілих держав. Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці співробітників банку, впровадити нові фінансові продукти і технології. Однак прогрес в техніці злочинів йшов не менш швидкими темпами, ніж розвиток банківських технологій. В даний час понад 90% всіх кіберзлочинів у банківській системі пов'язано з використанням автоматизованих систем обробки інформації банку (АСОІБ) [2]. Захист власне банківської системи повинен використовувати потужні засоби аутентифікації і контролю дій як внутрішніх користувачів, так і клієнтів. Загальноприйнято, що найбільш надійний захист можуть забезпечити кошти двофакторної аутентифікації, будь то електронні ключі (Токени) або генератори одноразових паролів. Безпека даних при зберіганні вимагає використання засобів шифрування, які зможуть працювати або на рівні сховищ даних, або на рівні окремих компонентів системи, наприклад, таблиць баз даних. Безпека банкоматів і платіжних терміналів повинна забезпечуватися з використанням традиційних засобів - антивірусного захисту.

Для забезпечення адекватності системи протидії інформаційним злочинам доцільно застосовувати принципи Ризик-менеджменту. Даний метод дозволить, при грамотному підході визначити і класифікувати загрози і, відповідно, до ймовірнішого настання негативних наслідків для банку, організовувати систему захисту. На жаль, на сьогодні принципи Ризик-менеджменту в сфері захисту інформації ще не дуже досконалі [89, с.5]. На практиці забезпечення інформаційної безпеки відбувається в умовах випадкового впливу чинників, які в повній мірі складно передбачити заздалегідь при проектуванні системи захисту інформації, але в подальшому

вони здатні знизити ефективність передбачених проектом заходів інформаційної безпеки або повністю скомпрометувати їх.

Однією з істотних проблем при проектуванні та експлуатації систем захисту інформації є ігнорування методології системного аналізу щодо засобів і інструментів для їх захисту. Слід визнати складність, а інколи і неможливість об'єктивного підтвердження ефективності системи захисту інформації, що в основному визначається неповнотою нормативно-методичного забезпечення інформаційної безпеки, перш за все в області показників і критеріїв [5]. Міжнародний стандарт для операцій з чіповими банківськими картами (EMV), введений в 2005 році, визначає фізичну, електронну та інформаційну взаємодію між банківською картою і платіжним терміналом для фінансових операцій на основі стандартів ISO / IEC 7816 для контактних карт, і ISO / IEC 14443 для безконтактних карт.

Інтернет-банкінг широко поширився серед банків і клієнтів. Використання Інтернет-ресурсів в якості альтернативного засобу передачі пін-коду клієнта в банк не тільки призводить до зниження витрат на передачу, а й дозволяє поліпшити банківську конкурентоспроможність і збільшити гнучкість роботи банку з клієнтами. Головними перешкодами на шляху інтернет-банкінгу є безпека системи, відсутність довіри і правової підтримки. Однак, безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту для всіх структурних елементів виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи об'єднуються в єдиний цілісний механізм - систему захисту інформації (СЗІ). При цьому функціонування системи має контролюватися, оновлюватися і доповнюватися в залежності від зміни зовнішніх і внутрішніх умов.

Саме тому, забезпечення безпеки банківської інформації, а також формування необхідних і достатніх умов для створення принципово нового методологічного базису, спрямованого на досягнення синергетичного ефекту

в сфері безпеки державних і приватних комерційних систем банківського захисту, є першочерговим завданням у протидії кіберзлочинам.

Діяльність АБС забезпечується і регулюється на основі законодавчих актів і рекомендацій Національного банку України, які були розглянуті у першому розділі. Проведений аналіз законодавчої бази України показав, що для забезпечення захисту інформації в АБС використовуються системи управління інформаційною безпекою (СУІБ), які забезпечують контроль за функціонуванням комплексних систем захисту інформації.

Таким чином, АБС є комплексною інформаційною банківською системою, що інтегрує різні сфери діяльності банку, здатної автоматизувати і об’єднати в єдині цілі бізнес-процеси фінансової установи. Комплексна система, що підтримує централізовану обробку, мультивалютність і автоматизацію основних фінансових операцій, повинна забезпечувати ефективне управління, контроль, отримання звітів про поточної діяльності всіх філій банку.

Серед функцій, властивих сучасним комплексним АБС, можна виділити наступні: операційний день; операції на фондовому ринку, робота банку з цінними паперами; роздрібні банківські послуги; дистанційне банківське обслуговування; електронні банківські послуги; розрахунковий центр і платіжна система (карткові продукти); інтеграція бек-офісу банку з його зовнішніми операціями; управління діяльністю банку; програми лояльности клієнтів, маркетингова, рекламна та PR-служби.

Приведені основні функції АБС реалізують наступні технології:

системи управління базами даних;

реалізація баз сховища даних, OLAP- і OLTP-технології обробки даних (системи оперативної аналітичної обробки і системи оперативної обробки транзакцій);

системи пошуку, вилучення та підготовки достовірних даних;

створення реального інформаційного простору банку, включаючи філії, клієнтів і партнерів;

безпечне підключення інформаційної системи банку до зовнішніх обчислювальних мереж (Інтернет);

організація безпечної, достовірної передачі даних по загальнодоступних каналах зв'язку (криптографія: шифрування і електронний цифровий підпис (ЕЦП), організаційні заходи), електронний документообіг;

технічне, програмне, математичне і інше забезпечення;

інформаційна аналітика і системи підтримки прийняття рішень (decision support systems, DSS);

захист інформації, що зберігається і оброблюваної інформації, всієї АБС в цілому;

системи віддаленої роботи з фондовими ринками і програми передбачення поведінки курсів;

розмежування доступу до інформації різного рівня секретності;

антивірусний захист;

інтернет-магазини і інтернет-картки;

центри обробки викликів (call-центри) і IP -телефонія;

підтримка різних каналів доступу: Інтернет, телефон, мобільна мережа, SMS, WAP і ін .;

підтримка і дослідження в області планомірного інформаційного розвитку АБС.

Основою комплексної АБС є банківська інформація – сукупність відомостей, пов'язаних з Статутними документами і Керівництвом банківської установи, організаційно-правовою формою банківської установи, нинішнім виглядом банківської установи і його службовців, видами і формами банківського обслуговування, кількістю і складом клієнтів, операціями по рахунках клієнтів, наявністю кореспондентських відносин і технічним забезпеченням банку [8].

На рис. 2.10 приведена загальна класифікація банківської інформації.

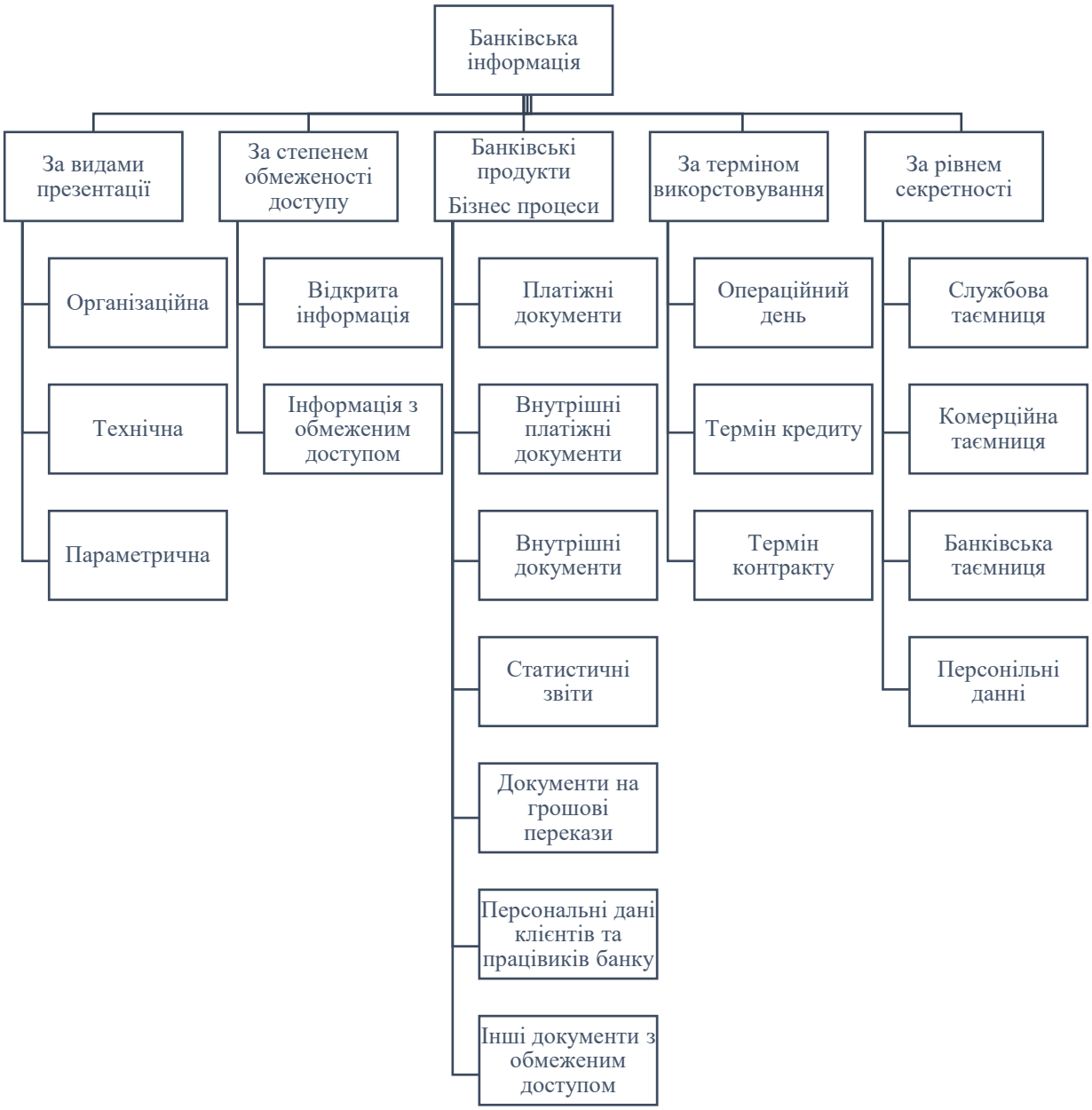

Рис. 2.10. Загальна класифікація банківської інформації

Перевагою запропонованої класифікації банківської інформації є те, що вона на відміну від відомих класифікацій дозволяє розкрити глибину змісту щодо суті даної категорії. Наприклад, за видами банківська інформація буває організаційною, технологічною та параметричною. При цьому під організаційною банківською інформацією слід розуміти інформацію, яка буде розкривати характер ділових зв’язків банку з клієнтами, інформацію про особливості організації та побудови системи управління банком.

Технологічна банківська інформація - це інформація про принципи управління банком при здійсненні ним усіх видів банківської діяльності, а також інформація про застосовування в системах банківського захисту новітніх високотехнологічних розробок. Параметрична банківська інформація - це інформація, яка відображає кількісні показники, що відображають банківський капітал і величину його кредитного портфеля при здійсненні банком всіх видів діяльності. Ще однією перевагою запропонованої класифікації є те, що в разі появи нових ознак, що характеризують ті чи інші аспекти категорії «банківська інформація» в запропонованій класифікації, передбачена можливість розширення безлічі ознак.

З запропонованої класифікації також випливає висновок про те, що в підсистемах АБС Банку циркулює інформація різних рівнів конфіденційності (секретності) від відкритої інформації, до відомостей, що містять інформацію з обмеженим доступом (комерційна, банківська і службова таємниця).

У документообігу АБС Банку також присутні: платіжні доручення та інші розрахунково-платіжні документи, звіти (фінансові, аналітичні та ін.), відомості про особові рахунки, узагальнена інформація та інші конфіденційні (обмеженого поширення) документи і т.д., які також можуть бути віднесені до поняття банківської інформації.

Таким чином, в найзагальнішому вигляді під банківською інформацією можна розуміти інформацію, яка виникає в результаті банківської діяльності. Це, перш за все відомості, що характеризують сам банк, його фінансове становище, надійність і виконання вимог законодавства. Таку інформацію можна отримати із статуту банку, його ліцензій, бухгалтерських балансів, звітів про прибутки і збитки та інших джерел.

Крім того, в більш вузькому розумінні банківська інформація – це відомості про конкретні операції банку. Така інформація характеризує не тільки банк, але і тих осіб, з якими банк вступає в правовідносини. Як приклад банківської інформації можна навести відомості про наявність

рахунків або вкладів і про операції по них, про майно, що знаходиться на зберіганні в банку.

Для аналізу основних видів загроз безпеці банківської інформації використамо відому модель безпеки – тріади CIA (confidentiality, integrity, availability) в трьох сферах (профілях) безпеки: інформаційної безпеки, безпеки інформації та кібернетичної безпеки.

У даній моделі під інформаційною безпекою розуміється процес забезпечення конфіденційності, цілісності та доступності інформації клієнтами / клієнтом банку на основі сукупності колективної та індивідуальної свідомості. У моделі під конфіденційністю розуміється забезпечення доступу до інформації тільки авторизованим користувачам, під цілісністю – забезпечення достовірності і повноти інформації, і методів її обробки для авторизованих користувачів, під доступністю – забезпечення доступу до інформації та пов’язаним з ній активів авторизованих користувачів в міру необхідності.

Безпека інформації – стан захищеності даних, при якому забезпечуються їх конфіденційність, доступність і цілісність.

Безпека інформації визначається відсутністю недопустимого ризику, пов’язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на дані і (або) на інші ресурси автоматизованої інформаційної системи, що використовуються в автоматизованій системі.

Кібербезпека – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберпростору, ресурсів організацій і користувачів. Кібербезпека передбачає досягнення і збереження властивостей безпеки у ресурсів організації або користувачів, спрямованих проти відповідних кіберзагроз. Кібербезпека охоплює такі поняття, як захист персональної інформації, а саме виявлення, запобігання або реакція на атаки. Стандарт ISO / IEC 27032 до: 2012 Information technology – Security techniques – Guidelines for cybersecurity – дає

чітке розуміння зв’язку терміна cybersecurity (кібербезпека) з мережевою безпекою, прикладною безпекою, Інтернет-безпекою та безпекою критичних інформаційних інфраструктур (рис. 2.11).

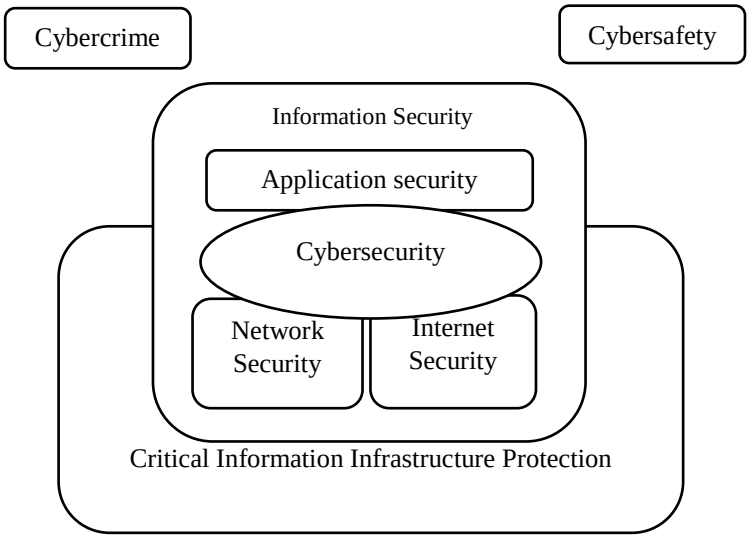

Рис. 2.11. Взаємозв’язок між кібербезпекою і іншими доменами безпеки

Таким чином, відома модель тріади CIA для комплексних АБС може бути представлена в вигляді, представленому на рис. 2.12.

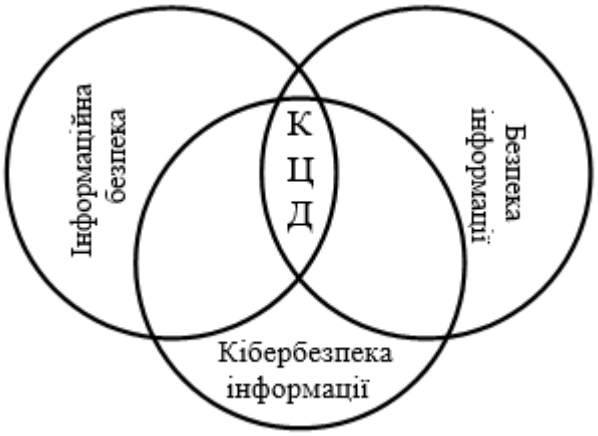

Рис. 2.12. Модель тріади CIA для комплексних АБС

Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту АБС схильна до різних загроз. Загрози

банку – потенційно можливі або реальні дії зловмисників або конкурентів, здатні завдати банку матеріальної чи моральну шкоду [36, с.102].

За походженням джерел загрози виділяють: внутрішні і зовнішні. Як перші, так і другі за спрямованістю і характером впливу на діяльність банків можуть бути економічними, фізичними та інтелектуальними.

До економічних загроз відносяться: корупція, шахрайство, недобросовісна конкуренція, використання банками неефективних технологій банківського захисту. Реалізація таких загроз веде до заподіяння збитків банкам або упущення ними вигоди.

Фізичні загрози: крадіжки, грабежі майна і коштів банків, поломки, виведення з ладу обладнання банків, неефективна його експлуатація. Внаслідок реалізації таких загроз наносяться збитки банкам, пов’язані з втратою своєї власності і необхідністю нести додаткові витрати на відновлення засобів захисту та інших матеріальних засобів.

Інтелектуальні загрози: розголошення або неправомірне використання банківської інформації, дискредитація банку на ринку банківських послуг, різного роду соціальні конфлікти навколо банківських установ або у середині банку. Наслідками таких загроз є: збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установи банків або в їх колективах.

Однією з найбільш вразливих місць в комплексній АБС є пересилання платіжних та інших повідомлень між банками, між банком і банкоматом, між банком і клієнтом, що пов’язано з наступними особливостями:

- внутрішні системи організацій відправника і одержувача повинні бути пристосовані для відправки та отримання електронних документів і забезпечувати необхідний захист при їх обробці всередині організації (захист кінцевих систем);

- взаємодія відправника і одержувача електронного документа здійснюється опосередковано через канал зв’язку.

Ці особливості породжують такі проблеми:

- взаємне пізнання абонентів (проблема встановлення взаємної автентичності при встановленні з'єднання);

- захист електронних документів, переданих по каналах зв'язку (проблеми забезпечення конфіденційності і цілісності документів);

- захист процесу обміну електронними документами (проблема докази відправлення і доставки документа);

- забезпечення виконання документа (проблема взаємної недовіри між відправником і отримувачем через їхню приналежність до різних організацій і взаємної незалежності).

Такий еволюційний ріст високих технологій в банківській сфері породжує пропорційне зростання кібератак із комп'ютерною грамотністю зловмисників в останні десятиліття, що в свою чергу призводить до вдосконалення відомих кібератак і появу нових видів загроз банківській діяльності.

А тому, основою управління інформаційною безпекою АБС є аналіз ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам.

Зазвичай виділяють дві основні групи методик розрахунку ризиків безпеки. Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності визначеному набору вимог щодо забезпечення інформаційної безпеки. Друга група методик оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. В даному випадку значення ризику обчислюється окремо для кожної атаки і в загальному випадку вираховується як добуток імовірності проведення атаки на величину можливого збитку від цієї атаки. Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту.

Основним недоліком переважної більшості сучасних комерційних систем виявлення аномалій (СВА) є відносно низька ефективність виявлення невідомих класів кібератак [10 – 12]. При цьому більшість сучасних СВА

використовують на базовому рівні ту чи іншу реалізацію технології сигнатурного методу виявлення кібератак, що сама по собі передбачає організацію процесу захисту з запізненням. Загалом виділяють два класи методів виявлення кібератак: методи виявлення аномалій і методи виявлення зловживань. В обох випадках вхідними даними для роботи системи виступають сформовані на основі безлічі вхідних параметрів шаблони поведінки – патерни подій. Завдання виявлення кібератаки при такій постановці зводиться до розпізнавання шаблона поведінки системи і фіксації факту її початку. Але, як і в першому, так і у другому випадках безліч вхідних параметрів підлягає оцінюванню на предмет їх інформативності.

Тому, з огляду на різну природу загроз для обраних профілів забезпечення банківської безпеки та в інтересах отримання в подальшому оцінок величини ризику еквівалентного грошовому капіталу, пропонується використовувати методики, засновані на комплексному підході до оцінки ризиків, що поєднує кількісні та якісні методи аналізу, до таких відносяться методики CRAMM і FAIR.

Методики комплексного підходу оцінки ризиків, як правило, використовують такі стадії:

- на першій стадії аналізується все, що стосується ідентифікації та визначення цінності ресурсів системи: визначення меж досліджуваної системи: відомості про конфігурацію системи, відомості про відповідальних осіб за фізичні і програмні ресурси, визначення кількості користувачів системи, їх привілеї. Проводиться ідентифікація ресурсів: фізичних, програмних і інформаційних, що містяться всередині кордонів системи, будується модель інформаційної системи з позиції ІБ;

- на другій стадії ідентифікуються загрози і оцінюються рівні загроз для груп ресурсів і їх вразливостей, оцінюються залежність призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і вразливостей, обчислюються рівні ризиків і аналізуються результати. В кінці

стадії замовник отримує ідентифіковані і оцінені рівні ризиків для своєї системи;

- третя стадія дослідження полягає в пошуку адекватних контрзаходів – пошук варіанту системи безпеки, найкращим чином задовольняє вимоги замовника. На цій стадії генерується кілька варіантів заходів протидії, адекватних виявленим ризикам і їх рівнів.

У контексті підвищення ефективності функціонування СВА, незважаючи на переваги і недоліки кожного з напрямків, вони обидва залишаються актуальними, а тому і інтенсивно розвиваються. Альтернативою є подальший розвиток класифікаторів кібератак, в основу яких покладені дерева прийняття рішень. Останні, при умови правильності їх побудови, дають можливість отримати досить достовірні результати класифікації і, що характерно, мають відносно низьку обчислювальну складність. Важливу роль у процесі класифікації кібератак відіграють вхідні дані, які виступають основою для побудови класифікаторів СВА комунікаційних систем. Саме тому, доцільним вбачається застосування загальнодоступної і широко відомої бази даних KDD99, яка дозволяє отримувати кількісну характеристику кібератак, а також їх якісну оцінку, що забезпечить захист від нових видів кібератак.

Таким чином, групування двох відомих підходів дозволить об’єднати переваги кожного з них, що надаються ними окремо, і при цьому відкриє можливості отримання як кількісних, так і якісних їх характеристик для ефективної організації систем захисту.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. У сучасних умовах в Україні існує проблема недосконалої правової регламентації та реалізації кримінальної відповідальності за вчинення кіберзлочинів, неефективної діяльності органів державної влади, до повноважень яких входить протидія кіберзлочинам, тощо.

В Україні правові основи системи кіберзахисту банківської системи знаходяться на початковому етапі розвитку

2. Банківська система як особливо вразлива до кіберзлочинності сфера є недостатньо захищеною та потребує вдосконалення діяльності банківських структур щодо протидії кіберзлочинам, поліпшення міжбанківської співпраці та взаємодії з правоохоронними органами.

3. Кібербезпека банків вимагає комплексного, чітко спланованого, поетапного вдосконалення систем її захисту.

Визначення принципів і форм взаємодії правоохоронних органів зі службами безпеки банків, розроблення відповідних методик документування і викриття злочинів дадуть змогу належно організувати боротьбу зі злочинами, вчиненими у кіберпросторі.

4. В Україні за 2017 рік кібершахраями було вкрадено 670 млн грн., при тому що у 2016 році майже удвічі менше – 339 млн грн. Це свідчить про те, що заходи кібербезпеки, організовані у банках, не є досить ефективними. Хоча дану проблему широко популяризують через засоби масової інформації, проводиться роз’яснювальна робота з даного питання серед населення, але випадки шахрайств все одно зростають.

5. Здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми

кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства.

6. В результаті проведеного аналізу виявлено, що збитки банків в результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує застосування методів Data Mining та розвинутих інформаційних технологій.

РОЗДІЛ 3
ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗЛОЧИНАМ У БАНКІВСЬКІЙ СФЕРІ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

3.1. Проблемні аспекти протидії кіберзлочинам у банківському секторі та можливі шляхи їх вирішення

На думку багатьох фахівців, спеціальні заходи протидії злочинності у сфері банківської діяльності, являють собою сукупність заходів, безпосередньо спрямованих на усунення не стільки загальних причин злочинності, скільки детермінантів конкретних злочинних проявів, що утворюють певний сегмент злочинності.

Попередження злочинності заходами економічного, соціального, політичного та культурно-виховного характеру досягається в основному за рахунок загального соціального попередження, при цьому аналогічні за змістом запобіжні заходи теж можуть здійснюватися (принаймні, активно ініціюватися) в рамках спеціально-кримінологічної діяльності.

На спеціально-криміналістичному рівні попереджувальну діяльність в умовах ринкової економіки та розвитку приватної власності безпосередньо здійснюють самі суб’єкти фінансово-кредитної системи, в першу чергу, силами і засобами своєї служби безпеки. Бо саме на них власники і вищий менеджмент фінансово-кредитних установ покладають вирішення комплексу завдань щодо забезпечення безпеки підприємницької діяльності з охорони власності від протиправних посягань.

Таким чином, служби безпеки стають ключовим інструментом у системі комплексної безпеки і захисту власності фінансово-кредитної установи, створення якої здійснюється виключно за ініціативою і при безпосередній участі його власника. До спеціально-кримінологічних заходів

попередження, здійснюваних безпосередньо учасниками даної установи можна віднести наступні:

1. Аналіз криміногенної ситупції в регіоні діяльності суб'єкта кредитно-фінансової системи.

2. Створення системи інформаційної взаємодії між суб'єктами фінансово-кредитної сфери.

3. Організація взаємодії між органами внутрішніх справ і суб'єктами фінансово-кредитної системи для попередження і припинення злочинних посягань.

4. Навчання фахівців фінансово-кредитної системи ефективним прийомам протидії протиправним проявам [91].

На нашу думку, однією з головних завдань є створення системи інформаційної взаємодії між суб'єктами фінансово-кредитної сфери, що в сучасних умовах стає формою посилення міжрегіональної кооперації підприємництва і найважливішим спеціальним заходом попередження економічних злочинів.

Слід зазначити, що практично кожна служба безпеки суб'єкта фінансово-кредитної системи з використанням регіональних філій і представництв формує в більшій чи меншій мірі свою індивідуальну модель раннього оповіщення у відповідності до специфіки кредитної та інвестиційної політики і потреб клієнтів в певних фінансових послугах.

Для реалізації своєї мети – попередження протиправних діянь загальної для всіх суб'єктів фінансово-кредитної, виникає реальна можливість для їх взаємовигідної інформаційної взаємодії. Завдяки такій кооперації розширюються можливості отримання інформації за рахунок якої відбувається кількісне і якісне збільшення обсягу корисних даних, необхідних для детального і докладного аналізу.

Останнє особливо актуально в умовах розвитку міжрегіональних фінансово-промислових груп, посилення їх інтеграції між собою, з одного боку, і розширення міжрегіонального співробітництва між кримінальними

елементами, з іншого. Все це дозволяє завчасно отримувати відомості про нові протиправні посягання, не характерні для даного регіону чи сфери економіки і вивчити наявний практичний досвід.

Слід особливо відзначити, що створена таким чином об'єднана система раннього оповіщення не має державного регулювання, а будується і розширюється суто на добровільній основі. Тому необхідно враховувати, що при функціонуванні такої системи часто виникають проблеми, пов'язані с достовірністю інформації, а також підставами її внесення. Необхідно відзначити, що організація взаємодії між органами внутрішніх справ і суб'єктами фінансово-кредитної системи для попередження і припинення злочинних посягань є також необхідною адже часто являється єдиним законним засобом припинення вже розпочатого злочинного посягання.

У регіонах у ряді випадків існують угоди між банками і місцевими правоохоронними органами. Загальним недоліком цих угод є відсутність чітких і конкретних положень про практичні форми, методи взаємодії, а також відповідальності відповідних керівників органів внутрішніх справ за бездіяльність у випадку надання недостовірної інформації про підготовлюваний злочин.

Одним з першорядних завдань спеціально-кримінологічного попередження злочинності в сфері банківської діяльності є, на наш погляд, оптимізація банківської системи, оскільки підвищення кримінальної активності у зазначеній сфері багато в чому пояснюється недостатнім рівнем розвитку банківського сектора і ринку банківських послуг.

Саме тому, в середині банку доцільно застосовувати такі етапи алгоритму виявлення кібершахрайства [110, с.85]:

 виникнення факту кіберзлочину в кредитній організації (банку);

 проведення перевірки працівниками банку або лабораторіями МВС, або найманими компаніями, що спеціалізуються на кіберзлочинах;

 проведення допиту штату співробітників кредитної організації, які відзначаються поведінкою або нехтуванням посадовими повноваженнями і інструкціями;

 терміново опечатується і вилучається комп'ютер, який безпосередньо має відношення до розкрадання грошових коштів. Після проведеного аналізу встановлюється причина, за допомогою якого виду кібератаки відбулося розкрадання і з якої адміністративної панелі нею управляли;

 в ході дослідження експерти виявляють псевдонім злочинця, його IP-адресу, чи було це злочинне угруповання і хто ж все-таки керував операціями щодо розкрадання грошей;

 звернення в правоохоронні органи з інформацією про вчинення злочину;

 надання заяви та звітних матеріалів службової перевірки з приводу розкрадання грошових коштів від кредитної організації, а також експертний висновок від фахівців з кіберзлочинів.

Важливо розуміти, як можна виявити і запобігти кіберзлочинам. Основними способами протидії загрозам є постійний моніторинг і своєчасне оновлення захисних систем.

На жаль, атаки найчастіше помічають через деякий час після їх початку, але до цього часу зловмисники вже встигають викрасти чималу суму грошей. Атаки на банківські організації готуються і плануються злочинцями довгий час – доходить навіть до одного року. Отже, спроби хакерів зламати систему безпеки банку потрібно намагатися ідентифікувати на самому ранньому етапі підготовки кібератаки, щоб уникнути збитків як таких.

Величезну роль у протидії кіберзлочинцям грає зворотний зв'язок кредитно-фінансових організацій з організаціями, що спеціалізуються на виявленні та усуненні кіберзагроз, а також з державними органами, які будуть виявляти та притягати злочинців до відповідальності. Тільки за

допомогою злагодженої, спільної роботи цих організацій можна знизити ризик кібератак на найраніших стадіях їх підготовки, а також оперативно нейтралізувати ті атаки, які зловмисникам все ж вдалося провести.

Знову ж правильним твердженням є неможливість протидії економічним злочинам, зокрема кібершахрайства, без взаємодії держав і міжнародних організацій, які здійснюють допомогу в запобіганні та боротьбі з кіберзагрозами. Щоб ефективно протистояти кіберзлочинцям, в державі необхідно вибудувати багаторівневу систему кібербезпеки, яка змогла б захищати і інтереси простих громадян, і державні або приватні організації [11].

Система кібербезпеки включає в себе ряд компонентів, таких як забезпечення фінансової і цифрової грамотності населення, допомога в поширенні серед громадян індивідуальних методів і спосіб захисту персональної інформації, а також механізми щодо попередження та протистояння кіберзагрозам.

Тому, можна запропонувати наступні заходи в боротьбі із кібершахрайствами, особливо соціальною інженерією:

1) доцільно побудувати алгоритми із використанням інструментів Data Mining, за допомогою яких відбуватиметься відслідковування операцій та перевірка їх на предмет шахрайства у відповідності з певними ознаками. Особливо дієвим є застосування нейронних мереж, що дозволить постійно налаштовувати систему на нові ознаки шахрайства. Тобто у випадку, коли шахрай знімає всю суму коштів з рахунку, то система здійснює перевірку даної операції. У випадку шахрайства операція блокується;

2) розробка автоматизованого модулю моніторингу, вбудованого в банківську систему та різні платіжні системи, функція якого – автоматична перевірка операцій на предмет шахрайства, блокування операцій та подвійна (потрійна) ідентифікація клієнта. Частково це реалізовано в існуючих платіжних системах, але у випадках соціальної інженерії системи не працюють. Коли система блокує операцію з ознаками шахрайства, то вона

повинна надіслати клієнту повідомлення, в якому вказується тип операції з вказівкою місця її здійснення та суми. Наприклад, якщо шахрай знаходиться в іншій країні, то клієнту надходить повідомлення, що є спроба зняття з його рахунку коштів на вказану суму із вказаної країни. Якщо клієнт не ініціював операцію, то він повинен надіслати банку код із відміною або з блокуванням;

3) створення інтегрованого банку даних, який буде містити інформацію щодо: способу, методу, виду шахрайства, характерних ознак, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв, тощо. Дана інформація дозволить формувати нові правила перевірки та контролю банківських операцій на предмет відповідності ознакам шахрайства. Подібні бази повинні створюватися не для окремих банків, а для всієї банківської системи, оскільки дана інформація є типовою;

4) жорстке обмеження прав доступу працівників банків до бази даних клієнтів для зменшення шахрайств з боку працівників. Це можливе за рахунок чіткого розмежування прав доступу до інформації, налаштованого на програмному рівні. Даний підхід потребує створення та модифікацію посадових інструкцій працівників банків та розробку інструкцій та рекомендацій головних банків та Національного банку України;

5) збільшити кількість інструментів соціальної роботи із населенням через засоби масової інформації та Інтернет для зменшення випадків соціального шахрайства. Це сприятиме формуванню ефективної системи взаємодії між банками та клієнтами [105, с.120].

Варто відмітити, що вже зараз багато кібератак – це комбінації різних методик і очевидно, в майбутньому цих загроз не стане менше. Використання тільки традиційних систем захисту банківської інформації не дає можливості адекватно захищатися від сучасних типів атак. Кредитні організації, які поставили блоки лише від відомих загроз, завжди ризикують, оскільки кіберзлочинці продовжують вигадувати і створювати нові техніки атак.

Тому, ще одним із способів вирішення цієї проблеми є формування спеціалізованого центру щодо забезпечення кібербезпеки в кредитно-

фінансовій сфері, який міг би оперативно реагувати на інциденти і координувати дії різних служб і організацій щодо запобігання і попередження протиправних дій. Подібні центри успішно функціонують у багатьох країнах, однак в Україні такої організації поки немає.

Національний банк України регулярно отримує звітність від кредитних організацій, в якій описуються відомості про виявлення інцидентів, пов'язаних з порушенням вимог щодо забезпечення захисту інформації при здійсненні переказів грошових коштів. Однак, з огляду на, те що проведення оперативно-розшукових заходів не входить у функції Національного банку України, така взаємодія з правоохоронними органами допомогла б краще розібратися у вразливості різних систем електронного банкінгу і підвищити якість виданих рекомендацій для кредитних організацій.

Наступна проблема, пов'язана із застосуванням електронного банкінгу, полягає в активному залученні даних систем до процесу легалізації злочинних доходів. Останнім часом відмивання грошей стало однією з основних міжнародних проблем, до вирішення якої залучені провідні країни світу.

Процедура відмивання грошей має вирішальне значення для функціонування практично всіх форм транснаціональної та організованої злочинності. Різні заходи економічного характеру, покликані виключити або обмежити можливість використання доходів отриманих незаконними шляхами, являють собою найважливіший і дієвий компонент програм по боротьбі зі злочинністю.

Наведемо лише деякі фактори, що сприяють відмиванню грошей:

- висока частка неофіційних доходів населення і бізнесу (існування паралельної економіки і / або «чорного ринку»);

- недосконаліть механізмів контролю та моніторингу за діяльністю кредитних організацій;

- недотримання міжнародних стандартів регулювання фінансової діяльності, розроблених спеціалізованими міжнародними організаціями.

Саме топ-менеджерам кредитних організацій необхідно добре розуміти, що клієнти комерційних банків, які використовують для виконання своїх операцій системи електронного банкінгу та займаються протиправною діяльністю, можуть не тільки нанести удар по репутації банку, але і створити для нього серйозні ускладнення у взаєминах з регулюючими органами, аж до відкликання ліцензії на здійснення банківських операцій.

Ще одна проблема пов'язана з вдосконаленням професійної підготовки персоналу банку (у тому числі працівникам служб внутрішнього контролю кредитних організацій) з питань забезпечення інформаційної безпеки. З огляду на помітне збільшення джерел банківських ризиків, основу яких складають особливості функціонування систем електронного банкінгу, фахівцям комерційних банків, в чиї функції входить управління ризиками, необхідно мати не тільки економічну або юридичну, а й технічну освіту, що дозволяє досить впевнено орієнтуватися в особливостях функціонування різних технологій ДБО.

Неналежне забезпечення інформаційної безпеки систем електронного банкінгу (зокрема, продаж населенню незахищених фінансових послуг) веде до створення передумов для розкрадання грошових коштів і фінансування криміналу. Існуюча динаміка розвитку сучасних процесів, пов'язана з ростом технічних можливостей, здатна багаторазово збільшити обсяги фінансування криміналу. Якщо допустити зростання рівня розкрадань у великих обсягах, це може бути серйозною загрозою економічній безпеці країни (табл. 3.1).

Отже, розглянуті проблеми мають в першу чергу практичне значення, так як спрямовані на вирішення важливого завдання для банківського бізнесу – підвищення довіри клієнтів кредитних організацій до технологій ДБО, включаючи системи електронного банкінгу.

Ще однією невирішеною проблемою у банківській діяльності є боротьба із кіберзлочинами направленими на платіжні системи, зокрема із використанням пластикових платіжних карток, які стають все більш масовим явищем в Україні. Вказана тенденція, зокрема, пов'язана із широким

розповсюдженням даного виду платіжних засобів, що у свою чергу, є результатом діяльності держави, спрямованої на поступове обмеження операцій із готівковими платежами (встановлення ліміту для готівкових платежів на рівні, що не перевищує 150 тис. грн.; заходи, спрямовані на протидію відмиванню коштів, отриманих злочинним шляхом, та ухилянню від сплати податків).

Таблиця 3.1

Актуальні напрями регулювання для банківського сектора [89, с.11]

напрями регулювання в умовах електронного банкінгу	завдання регулятора	завдання банку
Підвищення якості управління операційним ризиком в банках	Розробити і випустити рекомендації для кредитних організацій з управління операційним ризиком з метою мінімізації наслідків прояви джерел операційного ризику, пов'язаних з особливостями функціонування систем електронного банкінгу (як на стороні банку, так і на стороні клієнта)	Впровадити в системи управління ризиками в банку додаткові заходи щодо мінімізації наслідків прояви джерел операційного ризику в умовах електронного банкінгу. Адаптувати методики перевірок ризик-підрозділів і служби внутрішнього контролю до умов електронного банкінгу
протидія кіберзлочинам, що спрямовані на банки та їх клієнтів, в процесі використання систем електронного банкінгу	Розробити і випустити рекомендації для кредитних організацій щодо зниження ризиків, пов'язаних зі зростанням актив ності кіберзлочинців, чиї дії спрямовані на крадіжки грошових коштів як банків, так і їх клієнтів; Посилити взаємодію з правоохоронними органами для вироблення найбільш дієвих заходів щодо запобігання подібних злочинів. Створити центр з протидії кіберзагрозам в банківській сфері	Впровадити додаткові заходи захисту інформації для систем електронного банкінгу, грунтуючись на ризик-орієнтованому підході. Використовувати «кращу практику» в банку (грунтуючись на зарубіжному і вітчизняному досвіді) щодо запобігання кіберзлочинів
Використання систем електронного банкінгу в схемах, спрямованих на легалізацію злочинних доходів	Внести необхідні зміни до нормативних актів з метою підвищення «прозорості» операцій клієнтів банків в умовах ДБО, включаючи системи електронного банкінгу. Розробити і випустити рекомендації для кредитних організацій з виявлення «сумнівних» операцій, які виконуються з використанням систем електронного банкінгу	Впровадити заходи ідентифікації клієнтів, використовують для виконання своїх операцій системи електронного банкінгу. Розширити перелік ознак «сумнівних» операцій, які виконуються з використанням систем електронного банкінгу

Недостатня підготовка співробітників ризик-підрозділів банку по тематиці застосування технологій ДБО (включаючи системи електронного банкінгу)	Розробити і випустити рекомендації для кредитних організацій, спрямовані на підвищення якості підготовки фахівців ризик-підрозділів, служб внутрішнього контролю і підрозділів фінансового моніторингу з питань виникнення додаткових джерел ризиків, пов'язаних з особливостями функціонування систем електронного банкінгу	Впровадити заходи щодо підвищення рівня підготовки фахівців ризик-підрозділів, служб внутрішнього контролю і підрозділів фінансового моніторингу з питань, пов'язаних з особливостями функціонування систем електронного банкінгу. Це можуть бути додаткові курси щодо особливостей функціонування застосовуваних систем, перепідготовка «ризиковиків», що мають тільки економічне і / або юридичну освіту за програмами технічної освіти

Наведений перелік видів шахрайств та напрямів протидії таким шахрайствам не є виключним. Разом з тим, дослідження навіть основних напрямів протидії шахрайствам із використанням банківських платіжних карток, свідчить про те, що окремі із показників безпеки інформації можуть бути досягнуті виключно із застосуванням додаткових механізмів технічного захисту інформації, яка зберігається на банківських платіжних картках.

Одним із таких механізмів є використання чіп-модулів на банківських платіжних картках.

За підсумками проведеного аналізу виявлено, що поряд з очевидними перевагами застосування систем електронного банкінгу призвело до значного розширення профілю операційного ризику, активізації діяльності кіберзлочинців і використання даного виду ДБО для легалізації злочинних доходів.

Своєчасне прийняття регулюючими органами нормативних документів в області притрансформаційних змін електронного банкінгу сприятиме не тільки розвитку даного виду ДБО, а й підвищенню стабільності банківської системи.

Запропоновані підходи до регулювання електронного банкінгу спрямовані:

- на мінімізацію наслідків появи нових джерел операційного ризику в умовах електронного банкінгу, причинами чого є надійність апаратно-програмного забезпечення даного виду ДБО і надійність різного роду

провайдерів послуг (інтернет-провайдерів для систем інтернет-банкінгу та операторів стільникового зв'язку для систем мобільного банкінгу);

- на протидію кіберзлочинів в кредитно-фінансовій сфері, так як кіберзлочинність перешкоджає розвитку електронного банкінгу;

- на зниження ризику використання даного виду ДБО в схемах, призначених для легалізації злочинних доходів, за рахунок прийняття додаткових заходів щодо ідентифікації клієнтів, що застосовуються для виконання своїх операцій системи електронного банкінгу;

- на підвищення професійного рівня персоналу кредитних організацій, які обслуговують системи електронного банкінгу.

3.2. Міжнародний досвід попередження та запобігання кіберзлочинам у банківській діяльності і можливості його впровадження в Україні

На даному етапі розвитку системи захисту банківського сектору в Україні недостатньо розвинуті. Для забезпечення уникнення ризиків службам безпеки банків необхідно захистити бази даних і робоче обладнання персоналу, комп'ютерні мережі, термінали та банкомати від дій кіберзлочинців, а головне – своїх клієнтів. Тому заслуговують на увагу підходи іноземних держав до створення інституційних і технологічних передумов для протидії кіберзлочинності.

Аналізуючи ситуацію безпосередньо в різних країнах світу, спостерігаємо в основному посилення кіберзлочинності у фінансовій сфері. У 2017 р. через кіберзлочинців постраждали як мінімум 40 млн. американців, а також одна нафтова компанія, чиї відомості потрапили до хакерів. США, Китай, Японія і Німеччина щорічно втрачають близько 200 млрд дол. через кіберзлочини у банківській сфері. Втрати, пов'язані з особистими даними громадян, оцінюються в 150 млрд. дол. За статистикою відомої російської компанії Group-IB, що спеціалізується на розслідуванні комп'ютерних злочинів, обсяг російського ринку кіберзлочинності в 2018 р досяг 2,44 млрд дол.[73]

Комп’ютерні зловмисники в даний час зовсім не схожі на тінейджерів, які отримали початкові знання з хакерських web-сайтів. Це фахівці з досить високою підготовкою в області інформаційних технологій і у фінансових питаннях. Причому більшість з них діють у складі організованих злочинних груп. Доходи від комп’ютерних злочинів значно перевищують доходи, одержувані від продажу зброї і наркотиків.

За період з 2016-го по 2018-ий рік в цілому по світу спостерігалося зростання доходів кіберзлочинців, а до 2020 року передбачається послідовне зростання до 2 трильйонів долларів. Варто зазначити, що організації, які спеціалізуються на розробці захисту від посягань кіберзлочинців, постійно створюють і покращують свої захисні системи, які пропонують для використання фінансовими організаціями, але основна проблема полягає в часі виявлення і в здатності оперативно попереджувати загрози, а також вираховувати злочинців [73].

Найбільший обсяг розкрадань доводиться на США і країни ЄС, так як вони є найбільш фінансово та інвестиційно привабливими.

У 2018 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки [61, с.128]. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. Звіт був складений спеціально для того, щоб допомогти урядам та організаціям зрозуміти, наскільки вони кібернетично захищені в порівнянні з іншими країнами.

Базою для складання звіту були дослідження групи експертів у складі 80 фахівців з двадцяти семи країн. Вони надали компанії Security & Defence Agenda офіційні висновки про поточну готовність до кібератак інформаційних систем різних країн.

Крім групи експертів, до дослідження були залучені представники 250

світових лідерів у галузях ІТ-технології, інформаційної безпеки, захисту інформації, боротьби з кіберзлочинністю та ін. з 21 країни. Технологією дослідження передбачалося та було виконане їх анонімне опитування. За результатами роботи групи експертів та після обробки результатів опитування, Security & Defence Agenda провела ранжування та встановила рейтинг по 5-бальній системі. При цьому була досліджена поточна готовність до кібератак інформаційних систем 23 країн. Стан готовності для окремих країн був продемонстрований на прикладі рейтингу McAfee, який там використовується у якості основного засобу боротьби з кіберзлочинами (табл. 3.2).

Таблиця 3.2

Стан готовності до кібератак інформаційних систем окремих країн

<table>
<tr><td colspan="7">Бальна оцінка кібератакам</td></tr>
<tr><td>5</td><td>4,5</td><td>4</td><td>3,5</td><td>3</td><td>2,5</td><td>2</td></tr>
<tr><td rowspan="6">-</td><td rowspan="2">Ізраїль</td><td>Франція</td><td rowspan="2">Канада</td><td rowspan="2">Італія</td><td rowspan="2">Індія</td><td rowspan="6">Мексика</td></tr>
<tr><td>Нідерланди</td></tr>
<tr><td rowspan="2">Швеція</td><td>Німеччина</td><td rowspan="2">Японія</td><td rowspan="2">Польща</td><td rowspan="2">Латвія</td></tr>
<tr><td>Великобританія</td></tr>
<tr><td rowspan="3">Фінляндія</td><td>США</td><td rowspan="2">Австралія</td><td rowspan="2">Росія</td><td rowspan="3">Румунія</td></tr>
<tr><td>Іспанія</td></tr>
<tr><td>Естонія</td><td>Австрія</td><td>Канада</td></tr>
</table>

Найвищий результат, тобто 4,5 бали, було поставлено всього 3 країнам: Швеції, Ізраїлю та Фінляндії. Ще 8 країн, включаючи США, Великобританію, Францію та Німеччину, отримали друге місце з 4 балами. Росія та Польща зайняли 4 місце з 3-бальним результатом. З даних звіту Security & Defence Agenda, незрозуміло, чи були виставлені якісь бали для України [39].

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн

ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на ключові позиції.

Для України така тенденція є, в цілому, позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним. Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн [39], можна виділити об'єднуючі ключові позиції:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– визначення цілей інформаційних програм та затвердження їх у якості пріоритетних, покликаних прищепити користувачам нові моделі поведінки та

моделі роботи;

– доказ необхідності нової програми освіти в якій робиться акцент на навчання ІТ-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці.

Потреба реалізації ефективних заходів із протидії сучасним кібернетичним загрозам на національному рівні призводить до збільшення ролі в системах кібербезпеки країн спеціальних служб і правоохоронних органів, що мають контррозвідувальні функції й виконують завдання з протидії протиправній діяльності спецслужб іноземних держав і тероризму.

Аналізуючи системи кібербезпеки провідних країн світу, можна дійти висновку, що нині не існує уніфікованої моделі побудови національної кібербезпекової системи. Водночас важливим питанням залишається створення належної нормативно-правової основи для подальшої розбудови ефективних кіберспроможностей, закладення ключових підвалин національної кібербезпеки.

Так, натепер понад 50 країн світу мають стратегії кібербезпеки (в Україні подібною є Стратегія національної безпеки – авт.), які визначають ключові поняття кібербезпекової сфери, кіберзагрози, основні принципи побудови безпечного кіберпростору, напрями реалізації державної політики у сфері кібербезпеки, наголошують на важливій ролі державно-приватного партнерства та міжнародного співробітництва у сфері забезпечення кібербезпеки.

Поділяємо позицію, що одним із ключових питань організації ефективної роботи національних систем кібербезпеки залишається налагодження взаємодії між компетентними державними органами, які є суб’єктами кібернетичної безпеки, і здійснення координації з такої діяльності [40, с. 86].

Щодо зарубіжної практики протидії кіберзагрозам, зауважимо таке.

Розглядаючи країни Європи, приділимо увагу досвіду Великобританії, адже сьогодні в цій країні питання кібербезпеки виходять на першочергові

місця, що підтверджується тим, що у листопаді 2016 року Уряд Великої Британії оприлюднив 5-річний план реалізації Стратегії національної кібербезпеки і виділив на це 9 млрд. фунтів. Основним документом, спрямованим на забезпечення кібербезпеки у Великобританії, є Стратегія національної кібербезпеки 2016–2021 років, яку було прийнято замість аналогічної стратегії 2011–2015 років. Основна мета Стратегії на 2021 рік полягає в тому, щоб зробити Великобританію безпечною і стійкою до кіберзагроз, процвітаючою і впевненою в цифровому світі. Для цього необхідним є таке: 1) виділяти достатньо коштів для захисту Великобританії від розвитку кіберзагроз; ефективно реагувати на інциденти і забезпечувати захист і стійкість мереж і даних у Великобританії; 2) виявляти, розуміти, розслідувати ворожі дії, що вживаються проти Британії; 3) розробляти та сприяти розвитку інноваційних технологій та індустрії кібербезпеки [24].

Однак, незважаючи на великі витрати щодо забезпечення кібербезпеки та займаючи високі позиції щодо готовності до кібератак, Банк Англії (Bank of England) при моделюванні великої кібератаки проти британської фінансової системи виявився не готовим протистояти їй. Так, тест виявив деякі тривожні результати: багато хто з найбільших фінансових інститутів Великої Британії не готовий до великомасштабної онлайн-атаки на основі ідентифікаційної інформації (identity-based attacks). Дивує той факт, що багато хто з них також є неосвіченими в тому, як виявляти і повідомляти про порушення інформаційної безпеки. Газета The Telegraph UK повідомила, що навіть невеликі атаки призвели до серйозних порушень безпеки і падіння основних систем (Reeves, 2014). На цей час фінансові інститути, які пропонують банківські продукти на основі інтернет і мобільних послуг, стикаються дедалі з більшим тиском витончених шкідливих програм, фішингу і шахрайських дій. Адже Велика Британія, де сплата побутових послуг (47,6%) та фінансових послуг (27,3%) здійснюється за допомогою мобільного банкінгу, є найбільш привабливою площадкою для кібер-атак. Цей сегмент дуже активно розвивається й в Україні. Всі великі банки

пропонують клієнтам інтернет-банкінг: privat24, my.ukrsibbank, web-банкінг «Ощад 24/7» та ін., при цьому в Україні немає високоякісної системи управління інформаційною безпекою. Тому, українські банки також можуть стати «тренувальною ареною» для світової кіберзлочинності. Прийнята НБУ Постанова «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України», що визнає інформаційну безпеку як складову операційного ризику, котрий впливає на діяльність банку, стан його капіталу та якість менеджменту банку при визначенні рейтингової оцінки, беззаперечно відповідає світовим стандартам ведення банківського бізнесу, але навряд чи стане дієвим інструментом практичного захисту особистої інформації клієнтів та фінансових даних самих банків.

Інформаційна безпека – це багаторівнева система збору, зберігання, обробки, передачі та захисту інформації, що циркулює як у банку, так і зовні та може впливати на прийняття управлінських рішень відносно діяльності банку. У відповідності до значущості інформації та наслідків її розголошення можливо умовно поділити на інформацію front-офісів та interior-офісів. Інформація front-офісів зосереджена на даних клієнтів, на кількості та сутності послуг, що надає банк як в установі, так і за допомогою мобільного чи інтернет-банкінгу. Інформація interior-офісів – це аналітичні дані, що безпосередньо стосуються діяльності самого банку: його фінансові звіти, посадові інструкції, тонкощі відносин з різними клієнтами та контрагентами, фінансові плани, бюджети, стратегії розвитку та ін. Найчастіше ціллю кібератак є інформація front-офісів, за допомогою якої вони крадуть значні кошти клієнтів, тим самим наносячи шкоду не лише їм, але й репутації банку.

Відомий англійський фінансовий аналітик, старший віце-президент компанії Business Computing World UK Марк Рівз розробив 5 простих засобів запобігання кібератак на front-офіси, які успішно могли б бути використані у вітчизняній практиці, зокрема (Reeves, 2014):

1. Систематичне оцінювання ризиків онлайнових транзакцій на відповідність чуттєвості зміни інформації (тип клієнта, обсяг операції, якість обслуговування, мобільний засіб та ін.).

2. Підвищення стандартів аутентифікації інформації. Відмовитися від розповсюджених дворівневих методів ідентифікації прізвище-пароль на користь передових систем виявлення шахрайства на основі поведінки, які можуть автоматично виявляти транзакції або веб-сайт навігацій аномалії в реальному масштабі часу.

3. Застосування багаторівневого підходу до перевірки даних: нашарування різних, що доповнюють один одного технологій безпеки, таких, як сувора аутентифікація, поведінкове виявлення шахрайства поза зоною перевірки транзакції, мобільна перевірка справжності, розширена перевірка персоніфікації, SSL цифрові сертифікати.

4. Впровадження передових методів аутентифікації: перевірка мобільного на основі транзакцій, аутентифікації динамічних пристроїв − в тому числі одноразові сеансові куки і цифрові відбитки пальців та ін.

5. Підвищення рівня обізнаності та освіти клієнтів. Частину коштів банки повинні витрачати на розробку доступних освітніх проектів для своїх клієнтів. Це має подвійні наслідки: підвищення рівня безпеки та створення з клієнтами довготермінових партнерських відносин. Ці методи також можна застосовувати при захисті стратегічно важливої інформації для життєдіяльності та розвитку самого банку [20, с.23].

Наступна Європейська країна, досвіду якої ми приділимо увагу, є Німеччина, адже саме ця держава є однією з ключових країн, форми державно-приватного партнерства якої працюють як один з основних інструментів ефективної системи кіберзахисту країни. Однак останні декілька років у Німеччині спостерігається різке зростання кіберзлочинності. 2016 року кількість скоєних кримінальних діянь із використанням інтернет-технологій сягнула 82 649 випадків, тоді як у 2015 році поліція зареєструвала 45 793 кіберзлочини. Водночас дані кримінальної статистики вказують на

зростання показників розкриття таких злочинів. Загалом, кількість розкритих правопорушень такого типу зросла на 5,9 відсотка, досягнувши рівня в 38,7 відсотка. І така тенденція в державі продовжується і й досі. Через це А. Меркель наголосила, що кібербезпека має «надзвичайно вагоме значення». Вона зазначила, що уряд Німеччини актуалізував стратегію кібербезпеки. Крім того, федеральний уряд готовий співпрацювати з містами та громадами. Вона також закликала представників органів місцевої влади та підприємств звертатися до Федеральної служби безпеки у сфері інформаційних технологій у разі виявлення підозрілих випадків [64].

Як і у Великобританії, у 2011 Німеччині було прийнято Стратегію кібербезпеки Німеччини, відповідно до якої федеральний уряд застосовує заходи на основі вже створених структур до відповідних рівнів загроз за такими стратегічними напрямами: 1) захист найважливіших інформаційних інфраструктур; 2) ІТ-системи безпеки ФРН. Захист інфраструктур потребує більшої надійності ІТ-систем громадян, а також малих та середніх підприємств; 3) посилення ІТ-безпеки в публічному управлінні. Публічне управління ще сильніше захистить свої ІТ-системи; 4) для оптимізації оперативної співпраці всіх державних установ і покращення координації заходів щодо захисту проти ІТ-випадків було створено Національний центр кіберзахисту; 5) створено Національну раду кібербезпеки, діяльність якої спрямована на виявлення і усунення конструктивних причин криз - важливий превентивний інструмент у кібербезпеці; 6) ефективна боротьба зі злочинністю у кіберпросторі. Посилюються можливості правоохоронних органів, Федеральної служби безпеки у сфері ІТ й економіки в контексті подолання ІКТ-злочинності (стосовно захисту від шпіонажу і диверсій); 7) ефективна співпраця у кібербезпеці в Європі та світі. Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному і міжнародному рівнях; 8) використання надійних і достовірних інформаційних технологій. Потрібно забезпечити можливість доступу до надійних ІТ-систем і ІТ-компонентів/

Таким чином, у Німеччині досить багато уваги приділяється питанню забезпечення кібербезпеки, про що яскраво свідчить розгалужена система органів державної влади у досліджуваній сфері. Крім того, в державі активно застосовується міжнародне співробітництво, що дозволяє більш ефективно та оперативно виявляти загрози у досліджуваній сфері та розвивати вітчизняне законодавство і технології. Із позитивного також слід вказати на те, що в країні постійно відбувається розширення заходів, спрямованих на реалізацію державної політики у сфері забезпечення кібербезпеки.

Розглядаючи досвід Франції, зазначимо, що базовим нормативним актом, у якому визначаються стратегічні напрями державної політики Франції у сфері забезпечення безпеки, є Біла книга оборони та національної безпеки від 2008 р. та Національна стратегія цифрової безпеки 2015 р. Так, у Білій книзі серед найбільш ймовірних загроз територіям Франції та європейській спільноті (тероризм, використання балістичних ракет, організована злочинність, ризики природного характеру та ускладнення епідеміологічної ситуації у великих містах, прихована імміграція) названі: масштабні атаки на інформаційні системи банківських установ; шпіонаж та стратегічний вплив.

Що ж стосується Стратегії, то вона покликана супроводжувати цифровий перехід французького суспільства і відповідає новим викликам, викликаними зміною використання цифрових технологій і пов’язаних із ними загроз із п’ятьма цілями: 1) гарантувати національний суверенітет; 2) забезпечити сильну відповідь на акти кіберзлочинності; 3) інформувати громадськість в цілому; 4) забезпечити цифрову безпеку, адже це є конкурентною перевагою для французьких підприємств; 5) посилити позиції Франції на міжнародній арені. Відповідно до національної стратегії кібербезпеки, французька держава працює над забезпеченням безпеки IT-систем у напрямі колективного реагування, цифрової довіри, що є необхідним для стабільності держави, економічного розвитку і захисту громадян.

Таким чином, зміцнення стратегічної стабільності й міжнародної безпеки в кіберпросторі є однією з ключових цілей Франції. Тому вона відіграє активну роль у просуванні безпечного, стабільного і відкритого кіберпростору. Міністерство Європи і закордонних справ координує роботу Франції у сфері «кібер дипломатії». Франція особливо активна в межах ООН, де обговорюються правила відповідальної поведінки в кіберпросторі. Франція брала участь в останніх п'яти групах урядових експертів ООН (ЄСЕ) з кібербезпеки, чия робота допомогла розмістити кіберпростір у міжнародній системі, створеній Статутом Організації Об'єднаних Націй, і направляти держави до запобігання, співпраці й нерозповсюдження в кіберпросторі злочинності.

Досліджуючи зарубіжний досвід забезпечення кібербезпеки, не можна не звернути увагу на Польщу, яка сьогодні активно займається розвитком кіберзахисту на державному рівні. За прогнозами аналітиків, через два-три роки Польща буде лідером в ІТ-галузі в країнах Центрально-Східної Європи. Тривалий час зусилля влади Польщі щодо боротьби з кіберзагрозами були недостатніми. Однак низка масштабних атак на тлі відсутності єдиного координованого центру ухвалення рішень стали стимулом для наступних дій. По-перше, Польща ухвалила зміни до законодавства, які дозволяють запроваджувати у країні надзвичайний стан у разі атаки у віртуальному просторі. Такими юридичними новаціями можуть похвалитися небагато держав. По-друге, влада погодилася з недоцільністю функціонування кількох інституцій із боротьби з кіберзагрозами, які лише дублювали одна одну. У 2011 році було створено Міністерство адміністрації і цифровізації, завданням якого стало забезпечення кібербезпеки у військовій сфері, захист конфіденційності громадян, побудова національної освітньої платформи, залучення до інтернету людей похилого віку і жителів віддалених районів країни. По-третє, в межах Міністерства цифровізації у 2016 році створили Національний центр кібербезпеки. Його ключовим завданням стало попередження загроз, реакція на них та координація дій. Робота центру -

вдалий приклад державно-приватного партнерства у сфері кіберзахисту. Працює центр цілодобово. По-четверте, Польща опрацювала нову стратегію кібербезпеки. Вона передбачає, що до 2022 року влада гарантуватиме безпеку громадян, суб'єктів економічної діяльності і державних установ у галузі кібербезпеки [45].

Більш конкретними цілями вказаної стратегії є: 1) досягти здатності координувати дії на національному рівні, спрямовані на запобігання, виявлення, боротьбу та мінімізацію наслідків та/ або інцидентів, що порушують безпеку систем ІКТ, необхідних для функціонування держави; 2) посилення здатності протистояти кіберзагрозам; 3) підвищення національного потенціалу та компетенції в галузі безпеки в кіберпросторі; 4) формування сильної міжнародної позиції Республіки Польща у сфері кібербезпеки.

Якщо звернутися до досвіду Китаю, то стандартизація і державний контроль є основою безпеки Інтернету в країні, що дає правові можливості на законних підставах виявляти і документувати транснаціональні кіберзлочини.

Корисним для України є досвід країн Північної Америки, де відповідальність за втрати від шахрайства по карті несе її емітент. Так, відповідно до інструкцій Федерального резерву США, у разі виявлення факту незаконної діяльності з картковим рахунком і незалежно від суми збитку максимальну суму, що клієнт може заплатити, становить 50 дол., але більшість великих банків, як, наприклад, Bank of America, бере на себе 100% відшкодування за втрату коштів від шахрайства і, таким чином, несуть відповідальність за своє обладнання.

У країнах Євросоюзу передбачено різні види покарань за кіберзлочини. Наприклад, у Польщі викрадення платіжної картки карається позбавленням волі від трьох місяців до п'яти років, шахрайство у кіберпросторі – від шести місяців до восьми років, несанкціонований доступ до рахунків і персональних даних – від трьох місяців до п'яти років. В Іспанії

виготовлення фальшивих платіжних карток карається позбавленням волі від 8 до 12 років, а також штрафом у 10-кратному розмірі підробки.

За даними звіту консалтингової компанії PricewaterhouseCoopers (PwC), найбільш захищеними країнами є Малайзія, Японія та Індонезія.

Отже, як видно з проведеного аналізу більшість держав світу активно модернізує власні сектори безпеки відповідно до викликів сучасності, особливо зважаючи на потенціал використання мережі Інтернет у фінансових цілях. Цей процес відбувається з активним реформуванням систем управління відповідним сектором безпеки (створення спеціалізованих підрозділів, управлінських структур); упорядкуванням нормативного поля, що має забезпечити цілісність державної політики в цій сфері; активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз; збільшенням кількості підрозділів, зайнятих у системі кіберзахисту; розробленням кіберозброєнь і проведення пробних розвідувальних акцій у кіберпросторі; посиленням контролю за національним інформаційним простором (способами доступу, контентом тощо).

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам у кіберпросторі. До таких проблем передусім належать термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних і технічних продуктів іноземного виробництва, складнощі з кадровим наповненням відповідних структурних підрозділів.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Ключовим інструментом у системі комплексної безпеки і захисту власності фінансово-кредитної установи, створення якої здійснюється виключно за ініціативою і при безпосередній участі його власника є служби безпеки.

2. Велику роль у протидії кіберзлочинцям має зворотний зв’язок кредитно-фінансових організацій з організаціями, що спеціалізуються на виявленні та усуненні кіберзагроз, а також з державними органами, які будуть виявляти та притягати злочинців до відповідальності. Тільки за допомогою злагодженої, спільної роботи цих організацій можна знизити ризик кібератак на найраніших стадіях їх підготовки, а також оперативно нейтралізувати ті атаки, які зловмисникам все ж вдалося провести.

3. Ефективним способом протистояння кіберзлочинам є вибудова багаторівневої системи кібербезпеки, яка змогла б захищати як інтереси простих громадян так і державні.

4. Ефективними заходами в боротьбі із кібершахрайствами, особливо соціальною інженерією, могли б стати спеціально побудувані алгоритми із використанням інструментів Data Mining, за допомогою яких відбуватиметься відслідковування операцій та перевірка їх на предмет шахрайства у відповідності з певними ознаками. Особливо дієвим є застосування нейронних мереж, що дозволить постійно налаштовувати систему на нові ознаки шахрайства; розробленений автоматизований модуль моніторингу, який вбудований в банківську систему та різні платіжні системи, функція якого стала автоматична перевірка операцій на предмет шахрайства, блокування операцій та подвійна (потрійна) ідентифікація клієнта; створений інтегрований банк даних, який буде містити інформацію щодо: способу, методу, виду шахрайства, характерних ознак, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв, тощо. Дана інформація дозволить формувати нові правила перевірки та контролю банківських операцій на предмет відповідності ознакам шахрайства.

5. Наступним способом вирішення проблеми кіберзлочинності могло б стати формування спеціалізованого центру щодо забезпечення кібербезпеки в кредитно-фінансовій сфері, який міг би оперативно реагувати на інциденти і координувати дії різних служб і організацій щодо запобігання і попередження протиправних дій.

6. Аналізуючи системи кібербезпеки провідних країн світу, можна дійти висновку, що нині не існує уніфікованої моделі побудови національної кібербезпекової системи. Водночас важливим питанням залишається створення належної нормативно-правової основи для подальшої розбудови ефективних кіберспроможностей, закладення ключових підвалин національної кібербезпеки.

ВИСНОВКИ

Детальне дослідження протидії кіберзлочинам у банківській діяльності дозволяє зробити ряд висновків, які випливають із поставлених завдань:

1. Кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов’язане із використанням комп’ютерної техніки через комп’ютерні системи, або із комп’ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність.

Систему ознак боротьби із кіберзлочинністю визначено дворівнево. До загальних, тобто характерних явищу боротьби із злочинністю загалом, віднесено такі: 1) активність; 2) цілеспрямованість; 3) збірність; 4) комплексність.

2. Основними причинами розитку кіберзлочинності є:

- велика прибутковість – за оцінками Рахункової палати Сполучених

Штатів Америки, річний дохід злочинців лише від крадіжок і шахрайств, скоєних із використанням комп'ютерних технологій через Інтернет, сягає 5 мільярдів доларів;

- технологічні причини – це ті, які проявляються в технічній простоті вчинення кіберзлочинів;

- соціальні чинники є підґрунтям функціонування та розвитку кіберзлочинності. Передусім це зміни в суспільному житті, спричинені науково-технічним прогресом, пов'язані зі всебічною комп'ютеризацією суспільства, а також із формуванням інформаційного простору, заснованого на використанні комп'ютерів. У зв'язку із цим багато сфер соціальної активності переходять *у* віртуальний простір, що, *у* свою чергу, породжує нові проблеми – різні злочини з використанням електронно-обчислювальної техніки. І виникає необхідність у регулюванні цих проблем відповідним законодавством;

- політичні причини, які проявляються в недостатній обізнаності уряду країни щодо можливих суспільних наслідків кіберзлочинності. Через це скорочується бюджетне фінансування робіт зі створення правового, організаційного та технічного підґрунтя державної інформаційної безпеки, а також для захисту прав і свобод громадян, їхніх інтересів в інтернет-просторі. Також досить мало уваги приділяється правовому регулюванню комп'ютерної сфери, яка на тлі жорстокого та непідконтрольного розвитку призводить до деградації правових норм щодо потреб суспільства в інтеренет-просторі

3. Механізм правового регулювання боротьби з кіберзлочинністю – це чітко визначена й організована система юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

4. На сьогодні найбільш вразливою до кіберзлочинності є банківська система, яка недостатньо захищена та потребує вдосконалення діяльності банківських структур щодо протидії кіберзлочинам, поліпшення міжбанківської співпраці та взаємодії з правоохоронними органами.

5. В Україні за 2017 рік кібершахраями було вкрадено 670 млн грн., при тому що у 2016 році майже удвічі менше – 339 млн грн. Це свідчить про те, що заходи кібербезпеки, організовані у банках, є досить неефективними. Світовий досвід атак вірусів і значних фінансових втрат мав стимулювати, насамперед, саме фінансові установи до пошуку прогалин власних систем кіберзахисту та їх постійного оновлення. Однак 2017 рік показав фактичну неготовність українських банків захисти себе від подібних втручань у роботу їхніх інформаційних систем.

6. Загальна оцінка подій 27–29 червня 2017 року демонструє, що 70% українських банків так чи інакше постраждали від кібератак вірусу Petya. Видимим наслідком таких атак стала зупинка роботи терміналів, платіжних систем, відділень банків, а також обмежений доступ до інтернет-банкінгу та міжнародних переказів. Недооцінка потенційних загроз, відсутність належного програмного забезпечення та нехтування належним бюджетуванням систем кібербезпеки банку – все це свідчить про недостатність системного підходу до забезпечення кібербезпеки.

7. За інформацією Національного банку України, у банківській системі країни найбільш розповсюдженими є такі види кіберзлочинів: банкоматне шахрайство (скіминг, підробка платіжних карток, утручання в роботу банкомату під час здійснення операцій видачі готівки); шахрайство в торговельно-сервісних мережах (укладання фіктивних угод торговельного еквайрінгу, викрадення реквізитів платіжних карт, операції на суму нижче встановленого ліміту без про ведення авторизації, використання втрачених/ викрадених/підроблених платіжних карток); шахрайство в мережі Інтернет (проведення операцій із використанням викрадених реквізитів платіжних карток, створення фіктивних web-сайтів, поширення комп’ютерних вірусів та

троянських програм, перехоплення трафіку тощо); шахрайство в системах дистанційного банківського обслуговування (створення комп'ютерних вірусів та троянських програм для прихованого перехоплення управління комп'ютером клієнта, отримання платежів від закордонних відправників через міжнародну систему SWIFT унаслідок утручання у роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ).

8. Здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства.

9. В результаті проведеного аналізу виявлено, що збитки банків в результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує застосування методів Data Mining та розвинутих інформаційних технологій.

10. Для протидії кіберзлочинності та мінімізації нанесених збитків банківській установі та особам, яких вона представляє, банкам необхідно вдаютися до таких запобіжних заходів:

– ретельно перевіряти спеціалістів під час прийому на роботу;

– для захисту інформації вибирати сучасні інформаційні системи;

– користуватися послугами кваліфікованих комп'ютерних спеціалістів;

– займатися розробленням власних антихакерських програм;

– створити та постійно поповнювати власні бази даних осіб, що були причетними до скоєних кіберзлочинів;

– співпрацювати з іншими банками щодо обміну інформацією про злочинців, способи вчинення кіберзлочинів тощо.

11. Визначення принципів і форм взаємодії правоохоронних органів зі службами безпеки банків, розроблення відповідних методик документування і викриття злочинів дадуть змогу належно організувати боротьбу зі злочинами, вчиненими у кіберпросторі. У сучасних умовах в Україні існує проблема недосконалої правової регламентації та реалізації кримінальної відповідальності за вчинення кіберзлочинів, неефективної діяльності органів державної влади, до повноважень яких входить протидія кіберзлочинам, тощо.

12. В Україні правові основи системи кіберзахисту банківської системи знаходяться на початковому етапі розвитку. Пріоритетними напрямами забезпечення кібербезпеки банківської системи України є:

—моніторинг кіберпростору для своєчасного запобігання кіберзагрозам;

—захист інформаційних ресурсів банку з урахуванням практики розвинених країн світу;

—створення системи підготовки кадрів у сфері кібербезпеки в банках;

—розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки.

13. Основними чинниками, які відіграють ключову роль у боротьбі з кібезлочинністю та які пов’язані з діяльністю правоохоронних органів є:

- недостатнє забезпечення правоохоронних органів спеціальними технічними засобами, що допоможуть виявити та розслідувати кіберзлочини;
- технічна складність відстеження інформаційних загроз;
- відсутність належної взаємодії правоохоронних органів та приватного бізнесу з питань захисту комп’ютерних мереж, надання

необхідної інформації щодо порушень у віртуальному просторі;

- недосконаліть чинного кримінального та кримінально-процесуального законодавства .

14. Особливостями універсального міжнародно-правового регулювання боротьби з кіберзлочинністю є наступні: 1) відповідна діяльність акумулюється навколо ООН та її органів або створених за її підтримки суб'єктів; 2) на сьогодні наявні виключно програмні та інші стратегічні документи, які повинні закласти основи міжнародно-правового регулювання відповідного кола відносин; 3) основними напрямами діяльності має бути створення й розробка організаційних та законодавчих заходів протидії кіберзлочинності, а також питання взаємодії у даній сфері діяльності; 4) наявна необхідність у створенні міжнародних спільних органів оперативно-розшукової діяльності для забезпечення фіксування слідів вчинених злочинів; 5) удосконалення взаємодії між компетентними органами різних держав; 6) існує нагальна потреба розробки й прийняття універсальних конвенцій з відповідних питань, які би забезпечили участь більшості держав у відповідних заходах проти кіберзлочинності.

15. Особливостями нормативно-правової бази національного правового регулювання боротьби з кіберзлочинністю є наступні: 1) наявність системи національного правового регулювання боротьби з кіберзлочинністю, проте недостатній рівень єдності її елементів, що полягає у відмінностях в термінології, наявності розбіжностей у формулюваннях, прогалин та інших проблем; 2) комбінування у правовій системі норм вітчизняного законодавства та міжнародних правових актів, ратифікованих нашою державою; 3) наявність міжнародних договорів щодо двосторонньої співпраці у сфері правового регулювання боротьби з кіберзлочинністю; 4) існування Стратегії кібербезпеки України, що визначає подальший розвиток національного правового регулювання боротьби із кіберзлочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александров Ю. В. Кримінологія: курс лекцій. Київ: МАУП, 2002. 49 с.

2. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. Москва: Юридическая литература, 1991, 159 с.

3. Барташевська Ю. М. Оцінка ефективності витрат компанії на інформаційну безпеку. *Науковий вісник Міжнародного гуманітарного університету*. 2017. № 27. С. 87–90.

4. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. №6. С. 414–418.

5. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. Київ: Українська академія внутрішніх справ, 1994. 72 с.

6. Бойко В. О. Державно-приватне партнерство у сфері кібербезпеки. Київ: Національний інститут стратегічних досліджень, Відділ інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, 2018. 18 с.

7. Богославський М. Ю. Дослідження ступеню протидії банківським кібератакам на світовому та вітчизняному ринках. *Агросвіт.* 2018. № 2. С.88–92.

8. Бондаренко О. С. Рєпін Д. А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246–248.

9. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 94 с.

10. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформацій на безпека людини, суспільства, держави.* 2010. № 1 (3). 18 с.

11. Бухтіарова А. Г., Гуща А. В. Протидія кіберзлочинності у банківській сфері. *Приазовський економічний вісник.* 2019. № 3. С. 355–361.

12. Васильєв А. А. Пропозиції та зауваження до проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки». *Актуальні питання діяльності слідчих підрозділів органів внутрішніх справ України*: зб. наук. праць факультету з підготовки слідчих ХНУВС за 2012 рік / за заг. ред. чл.-кор. НАПрН України, д-ра юрид. наук С. М. Гусарова; академіка НАПрН України, д-ра юрид. наук, проф. О. М. Бандурки. Харків: Диса плюс, 2013. С. 599–602.

13. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. № 1(2). С. 276–283.

14. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия . Москва: Право и закон, 1996. 36 с.

15. Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования. *Правовые вопросы связи,* 2007. № 2. С. 17–25.

16. Войтенко І. С. Види шахрайств із використанням банківських платіжних карток та способи їх вчинення. Юридичний науковий електронний журнал. 2018. № 6. С. 332–335.

17. Волкова С. Шахрайство з картками: пастки для довірливих URL: https://minfin.com.ua/ua/2019/01/31/36553492/ (дата звернення: 31.01.2019).

18. Всемирный обзор экономических преступлений за 2016 год. *PricewaterhouseCoopers* URL: http://www.pwc.ru/. (дата звернення: 10.12.2016).

19. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності. І*нформація і право*. 2019. № 1. С. 118–128.

20. Гайдош Т. Киберпреступность преобретает индустриальный характер. *Финансы и развитие*. 2018. № 2. С. 22–27.

21. Гавловський В. Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право.* 2019. № 1. С. 108–117.

22. *Голина В. В.* Проблемы компьютерной преступности. Фінансова злочинність: зб. матеріалів міжнар. наук.-практ. семінару (м. Харків, 12–13 лютого 1999 р.). Харків: Право, 2000. С. 64–65.

23. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.

24. Головинов О., Погорелов А. Киберпреступность в современной экономике. *Вопросы инновационной экономики*. 2016. Т. 1, С. 73–88. DOI: 10.18334/vinec.6.1.35353. (дата звернення: 03.07.2019).

25. Гуцалюк М. В. Сучасні тенеденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1. С. 118–129.

26. Гуцалюк М. В. Протидія використанню учасниками злочинних угруповань мережі «Даркнет». *Інформація і право*. № 3(26). 2018. С. 102–108.

27. Даньшин И. Н. Общетеоретические проблемы криминологии: моногр. Харьков: Прапор, 2005. 55с.

28. Діордіца І. Поняття та зміст національної системи кібербезпеки. *Національний юридичний журнал: теорія і практика*. 2016. № 12. С. 37–42.

29. Діордіца І. Поняття та зміст кіберзлочинності. *Науковий вісник Херсонського жержавного університету.* 2017. № 3. С. 8–13.

30. Дементьева М. А., Лихачева В. В. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия. *Экономические отношения*. 2019. № 2. С. 1009–1019.

31. Добржанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин.* 2011. № 102 (1). С. 111–116.

32. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. URL: http://zakon2.rada.gov.ua/laws/show/994_687. (дата звернення: 21.07.2019).

33. Домінова І. В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Науково-виробничий журнал «Бізнес-навігатор».* 2017. № 4–2. С. 92–98.

34. Доусчі М. І. Правове регулювання забезпечення кібербезпеки в Україні. *Кібербезпека в Україні: правові та організаційні питання*: матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 30 листопада 2018 р. Одеса: ОДУВС, 2018. С. 21–23.

35. Дрьомін В. М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства: монографія. Одеса: Юридична література, 2009. 616 с.

36. Евсеев С. П. Синергетический подход к оценке безопасности банковских систем. *Системи обробки інформації*. 2016. № 4. С. 90–103.

37. Жердецька Л. В. Розвиток фінансових технологій: загрози та можливості для банків. *Економіка і суспільство*. 2017. № 10. С.583–588.

38. Журавленко Н. И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере. *Общество и право.* 2015. № 3 (53). С. 66–70.

39. Збитки від глобальних кібератак у світі сягнули $ 53 мільярдів – МВФ. URL: https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-mil.ardiv-mvf.html (дата звернення: 07.09.2019).

40. Згадзай О. Э. Киберпреступность: факторы риска и проблемы борьбы. *Вестник НЦ БЖД.* 2013. № 4 (18). С. 80–86.

41. Зелинский А. Ф. Криминология: курс лекций. Харьков: Прапор, 1996. 21 с.

42. Іванов Ю. Ф. Кримінологія: навч. посіб. 2-ге вид., доповн. та перероб. Київ: Вид. ПАЛИВОДА А. В., 2008. 60 с.

43. Іванченко О. Ю. Кримінологічна характристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 3. С. 172–177.

44. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение. *Власть*. 2014. № 8. С. 46–50.

45. Киберпреступники наживаются на самых бедных. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-o-time-to-waste-in-cybercrime-fight--says-un-chief. (дата звернення: 19.02.2019).

46. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnij-ploshchini-2014774.html. (дата звернення: 04.06.2019).

47. Кіберзлочинність: проблеми боротьби і прогнози URL: http://anticyber.com. (дата звернення: 11.06.2019).

48. Кіберполіція припинила діяльність одного з найвідоміших майданчиків у DarkNet із продажу персональних даних. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-odnogo-z-najvidomishyx-majdanchykiv-u-darknet-iz-prodazhu-personalnyx-danyx-4672 (дата звернення: 27.12.2018).

49. Клочко А. М.. Єременко А. О. Шахрайство з використанням банківських платіжних карток. *Юридичний науковий електронний журнал*. 2016. № 1. С.85–92.

50. Козлов Д. Н. Система предотвращения мошенничества как составляющая кредитного конвейера. *Банковское кредитование*. – 2013. – № 2 (48). – С. 15–25.

51. Комп'ютерна злочинність: навч. посіб. Київ : Атіка, 2002. 55 с.

52. Конвенція про кіберзлочинність від 23.11.2001 р. *Офіційний вісник України.* 2007. №65. С 25–35.

53. Кравцова М. А. Понятие киберпреступности и ее признаки. *Часопис Київського університету права.* 2015. № 2. С. 320–325.

54. Кривошапова С. В., Литвин Е. А. Оценка и способы борьбы с мошенничеством с банковскими картами. *Международный журнал прикладных и фундаментальных исследований.* 2015. № 4. С. 116–120.

55. Криминология: учеб. / под ред. проф. Н. Ф. Кузнецовой, проф. В. В. Лунева. – 2-е изд. Москва: Волтерс Клувер, 2004. 90 с.

56. Криминология: учеб. для вузов / под общ. ред. д.ю.н., проф. А. И. Долговой. 3-е изд. Москва: Норма, 2005. 68 с.

57. Криминология: учеб. для вузов / под ред. проф. В. Д. Малкова. – 2-е изд., перераб. и доп. – М. : Юстицинформ, 2006. – С. 32.

58. Криминология: учеб. для юридических вузов / под ред. проф. В. Н. Бурлакова. Санкт-Петербург: Санкт-Петербурская академия МВД России, 1998. 60 с.

59. Кришевич О. В. Способи шахрайства в банківській сфері: кримінально-правовий аспект. *Кримінальне право і кримінологія*. 2012. № 2 (23). С. 111–116.

60. Марків С. І. Кіберзлочинність. *Нова кримінальна загроза URL:* http://gurt.org.ua/articles/34602. (дата звернення: 20.10.2019).

61. Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. 2018. № 1. С. 127–132.

62. Мельник С. С. Класифікація фінансового шахрайства в комерційному банку. *Науковий вісник Херсонського жержавного університету.* 2017. № 3. С. 89–92.

63. Мельник С. С. Типологія фінансового шахрайства в українських комкрційних банках. *Вісник університету банківської справи*. 2017. № 1. С. 65–70.

64. Меркель: уряд Німеччини актуалізував стратегію кібербезпеки. URL: http://vgolos.com.ua/news/merkel_uryad_nimechchyny_aktualizuvav_strategiyu_kiberbezpeky_256173.html. (дата звернення: 03.02.2019).

65. Міщук Н. В. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету.* 2014. № 51. С. 173–179.

66. Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий.

Вестник Полоцкого государственного университета. 2011. № 14. С. 143–149.

67. Морозов Н. А. Борьба с компьютерной преступностью в Японии. *Общество и право*. 2014. № 2 (48). С. 141–145.

68. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою. *FINANCE.UA*. 2018. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly kibershahrayivna-pivmilyarda-yak-ne-staty-zhertvoyu. (дата звернення: 09.09.2019).

69. Номоконов В. А. Киберпреступность как новая криминальная угроза *Криминология: вчера, сегодня, завтра.* 2012. № 1 (24). С. 45–55.

70. Номоконов В. А. Киберпреступность: угрозы, прогнозы, проблемы борьбы. *Information Technology and Security*. 2013. № 1 (3). 88 с.

71. Номоконов В. А., Тропина Т.Л. Киберпреступность как новая криминальная угроза. *Криминология: вчера, сегодня, завтра*. 2012. № 1. С. 45–55.

72. Номоконов В. А., Тропина Т. Л. Киберпреступность: угрозы, прогнозы, проблемы борьбы. *Information Technology and Security*. 2013. № 1. С. 86–94.

73. Общемировые убытки от киберпреступности составят $2,1 трлн до 2019 года. URL : http://www.securitylab.ru/news/472924.php. (дата звернення: 15.04.2019).

74. Олійничук О. Банківські картки як обєкт шахрайства: стан і протидія явищу. *Актуальні проблеми правознавства*. 2017. № 1. С. 91–94.

75. Орлов О. В., Онищенко Ю. М. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю. *Теорія та практика державного управління*. 2013. № 3. С. 3–9.

76. Пархоменко С. В. Предупреждение компьютерной преступности в Российской федерации: интегративный и комплексный подходы. *Криминологический журнал Байкальского государственного университета экономики и права.* 2015. Т. 9, № 2. С. 265–276.

77. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник /за заг. ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

78. Пивоваров В. В., Терещенко К. В. Шахрайство з банківськими картками: окремі питання віктимології профілактики. *Карпатський правничий часопис*. 2015. № 10. С. 132–137.

79. Підсумки квартального засідання Форуму безпеки розрахунків з платіжними інструментами та кредитами 25 травня 2018р. *Украинская межбанковская ассоциация членов платежных систем ЕМА.* 2018. URL: https://ema.com.ua/summary-fbrik-may-2018. (дата звернення: 11.07.2018).

80. Погорецький М. А. Кіберзлочини: до визначення поняття. *Вісник прокуратури.* 2012. №8. С. 89-96.

81. Подосенков Н. С. Риски мошенничества в торговом финансировании Управление финансовыми рисками. 2015. № 4 (44). С. 270–277.

82. Поняття та сутність кібернетичної злочинності URL: http://legalactivity.com. (дата звернення: 20.05.2019).

83. Попова Т. В., Ліпкан В. А. Стратегічні комунікації: словник / за заг. ред. доктора юридичних наук В.А. Ліпка. 2016. 416 с.

84. Преступления, связанные с использованием компьютерной сети. *Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями.* URL: http://www.un.org/ russian/topics/crime/docs10.htm (дата обращения: 21.02.2019).

85. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19 (дата звернення: 07.09.2019).

86. Проблеми чинної вітчизняної нормативно-правової бази *у* сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка URL : http://www.niss.gov.ua/articles/454. (дата звернення: 04.12.2018).

87. Пфо О. М. Основні поняття і класифікація кіберзлочинності. Актуальні задачі та досягнення *у* галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., (м. Кропивницький, 23–25 листоп. 2016 р.). Кропивницький: КНТУ, 2016. С. 33–34.

88. Рассолов И. М. Право и Интернет. *Теоретические проблемы*. Москва: Норма, 2009. 383 с.

89. Ревенков П. Актуальные направления регулирования электронного банкинга. *Финансы и кредит*. 2015. № 24. С. 2–13.

90. Рогозин В. Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий. *Расследование преступлений: проблемы и пути их решения.* 2015. № 1 (7). С. 56-58.

91. Рудий Т. В., Сеник В. В., Рудий А. Т. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. *Науковий вісник Львівського державного університету внутрішніх справ*. 2018. № 1. С. 283–301.

92. Саяпин А. Предотвращение мошенничества в корпоративном бизнесе банка: практические аспекты. *Банковский менеджмент*. 2010. № 4. С. 14–18.

93. Словник термінів із кібербезпеки / ра заг. ред. О. В. Копана, Є. Д. Скулиша. Київ: ВБ «Аванпост-Прим», 2012. 214 с.

94. Статистика платежного мошенничества – итоги 2017-го года. *Украинская межбанковская ассоциация членов платежных систем ЕМА*. 2017. URL: https://ema.com.ua/cyberfraud-emastatistics-results-2017. (дата звернення: 09.08.2019).

95. Стратегія забезпечення кібернетичної безпеки України (Проект) URL : www.niss.gov.ua/public/File/2013_nauk.../kiberstrateg.pdf. (дата звернення: 16.10.2019).

96. Тарасов А. Электронный банкинг и его безопасность. *Экономическая политика.* 2010. № 5. С. 118–128.

97. Тихомиров О. О. Кіберзлочин: теоретико-правові проблеми: матеріали наук.-практ. конф., *«Інформаційна безпека: виклики і загрози сучасності»*. (5 квітня 2013 р.). Київ: Наук.-вид. центр НА СБ України. 2013. С. 179–182.

98. Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма. *Криминология: вчера, сегодня, завтра.* 2014. № 2 (33) С. 94–97.

99. У Великобританії створили реабілітаційний центр для кіберзлочинців. URL: http://ms.detector.media/web/cybersecurity /u_velikobritanii_ stvorili _reabilitatsiyniy_tsentr_dlya_kiberzlochintsiv (дата звернення: 08.04.2019.

100. У Німеччині різко зросла кіберзлочинність. URL: https://www.dw.com/uk/y-HiMe44HHi- Кіберзлочинність/a-38555191. (дата звернення: 08.04.2019).

101. Украинская аудитория Facebook выросла на 3 млн человек за 2018 год, общее количество пользователей соцсети в нашей стране составляет 13 млн. URL: https://itc.ua/news/ukrainskaya-auditoriya-facebook-vyirosla-na-3-mln-chelovek-za-2018-god-obshhee-kolichestvo-facebook-polzovateley-teper-sostavlyaet-13-mln-infografika/#disqus_thread (дата звернення: 19.02.2019).

102. Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы. *Молодые ученые.* 2012. № 3. С. 178–186.

103. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник.* 2018. № 3. С. 158–162.

104. Шевченко А. М. Зловживання та махінації на ринку фінансових послуг: методи боротьби, засоби протидії. *Глобальні та національні проблеми економіки*. 2015. № 7. С. 767–771.

105. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ ім. І. Вернадського.* 2018. № 29. С. 119–124.

106. Юрасов А. В. Основы электронной коммерции: учеб. Москва: Горячая линия-Телком, 2008. 165 с.

107. Як це робила Польща: досвід боротьби з кіберзагрозами. *Електронне видання «Економічна правда».* URL: https://www.epravda.com.ua/columns/2017/10/12/630044/ (дата звернення: 12.10.2019).

108. Яровенко Г. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=6453 (дата звернення: 12.10.2019).

109. Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Гроші, фінанси і кредит*. 2018. № 18. С. 836–841.

110. Яцик Т. П., Кисла К. О. Кіберзлочинність в Україні: аналіз дієвості способів розслідування кіберзлочинів і напрями їх удосконалення. *Юридичний науковий електронний журнал*. 2019. № 1. С. 183–186.