УДК: 336.71

КІБЕРЗЛОЧИННІСТЬ В БАНКІВСЬКІЙ СФЕРІ УКРАЇНИ

Лихопій В. І., ст. викладач
Полтавська державна аграрна академія

Статтю присвячено інформаційно-правовим аспектам регулювання кіберзлочинності як однієї з основних проблем інформаційного суспільства в сучасних умовах. Розглянуто нормативно-правову базу та важливі міжнародні документи, що регулюють суспільні відносини у сфері боротьби з кіберзлочинністю та кредитними шахрайствами. Висвітлено поняття кіберзлочинності, її складові та наслідки від здійснення, досліджено теоретичні проблеми боротьби з організованою кіберзлочинністю. Узагальнено головні види кіберзлочинів у банківській сфері та їх основні характеристики. Також наведено статистичні дані щодо стану кіберзлочинності в банківській системі України, на основі яких сформовано висновки та обґрунтовано необхідність розробки та втілення практичних рекомендацій щодо їх вирішення.

The article is devoted to information and legal aspects of the regulating of the cybercrime as one of the main problems of the information society in the modern world. We consider the regulatory framework and important international documents which regulate social relations in the struggle against the cybercrime and the credit fraud. We analysed the concept of cybercrime, its components and consequences of implementation, we researched the theoretical problem of combating organized cybercrime. We overview main types of cybercrime in the banking sector and their main characteristics. In the article was also presented statistics on the state of cybercrime in the banking system of Ukraine, where after the conclusion was formed on this basis and was found the necessity of developing and implementing practical recommendations for their solution.

Постановка проблеми. Сучасне суспільство у величезній мірі залежить від управління різними процесами за допомогою комп'ютерної техніки шляхом електронної обробки, зберігання і передачі інформації. Розвиток інформаційних технологій несе за собою не тільки позитивні, а й свої негативні тенденції та явища, пов'язані, зокрема, з появою нових видів злочинів з незаконним втручанням у роботу систем і комп'ютерних мереж, розкраданням і несанкціонованим доступом до баз даних та привласненням засобів, які сьогодні об'єднані під назвою «кіберзлочинність».

Боротьба з кіберзлочинністю і кредитним шахрайством залишається досить гострим питанням, яке потребує негайного вирішення.

Аналіз останніх досліджень і публікацій. Проблему кіберзлочинності досліджувало чимало вітчизняних і зарубіжних науковців. Серед них можна виділити праці Д. С. Азарова, П. Д. Біленчука, В. Б. Вєхова, В. І. Гаєнка, В. О. Голубєва, І. Ю. Карпушевої, М. В. Карчевського, В. В. Лісового, В. С. Цимбалюка, В. Г. Хахановського та інших.

Постановка завдання. Метою наукових досліджень у даній статті є теоретичне узагальнення поняття кіберзлочинності в банківській сфері, її видів та виявлення негативних наслідків даного явища. При цьому, необхідним є дослідження поточного становища кіберзлочинності та розробка окремих рекомендацій щодо поліпшення стану в даній сфері.

Виклад основного матеріалу дослідження. На сьогодні законодавство України є недосконалим у сфері боротьби з кіберзлочинністю. Наразі у вітчи-

зняному законодавстві не міститься чіткого визначення поняття «кіберзлочинності», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням мереж електрозв'язку та комп'ютерних систем. Незважаючи на відсутність загальноприйнятного визначення кіберзлочину, спостерігається досить широке та вичерпне розуміння його суті та способів його вчинення, а також загроз та ризиків, що дає можливість розробляти та запроваджувати заходи протидії даному виду злочину.

На державному рівні розроблені нормативно-правові документи, що регулюють систему фінансового моніторингу в сфері фінансових злочинів . До них відносять Закони України: «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму», «Про банки і банківську діяльність»; Кримінальний кодекс України, Кодекс України про адміністративні правопорушення; Конвенція про відмивання, пошук, арешт та конфіскацію доходів.

Зі змісту статей 361 – 363 розділу 16, а також деяких інших (ст. 185–191) Кримінального кодексу України, випливає, що під кіберзлочином розуміють діяльність, що пов'язана як з посяганням на встановлений порядок використання електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку, так і з замахом на інші об'єкти, де електронно-обчислювальні машини (ЕОМ) є інструментом досягнення злочинної мети.

Кримінальний кодекс України у Розділі XVI передбачає відповідальність за такі злочини, як несанкціоноване втручання в роботу ЕОМ; створення та розповсюдження шкідливих програмних чи технічних засобів; несанкціоноване розповсюдження інформації з обмеженим доступом, що зберігається в ЕОМ; несанкціоновані дії з інформацією, вчинені особою, яка має право доступу до неї; порушення правил експлуатації ЕОМ чи правил захисту інформації; перешкоджання роботі ЕОМ шляхом масового розповсюдження повідомлень електрозв'язку. Зазначені злочини, в залежності від виду та тяжкості, можуть каратись як штрафом (до 1000 неоподатковуваних мінімумів доходів громадян), так і позбавленням волі строком до шести років, при цьому конфіскуються програмні та технічні засоби, за допомогою яких було вчинено злочин [3].

Міжнародна спільнота перебуває у постійному пошуку заходів, що дозволяють мінімізувати негативні наслідки кіберзлочинності на суспільство. Останніми роками розробляється велика кількість міжнародних та регіональних положень, що спрямовані на протидію кіберзлочинності. Основні з них: Сорок рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF), Вісім Спеціальних Рекомендацій FATF, Директива Ради ЄС про запобігання використанню фінансової системи з метою відмивання грошей.

Одним з важливих міжнародних документів, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року, яка відображає загрози та небезпеки сучасному інформаційному суспільству.

Згідно до положень Конвенції, комп'ютерні правопорушення класифіковані на певні групи. Перша група передбачає кримінальну відповідальність за вчинення правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями. Друга група передбачає відповідальність за правопорушення, пов'язані з комп'ютерами, а саме: підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами. Третя група - правопорушення, пов'язані зі змістом, до яких відносять правопорушення, пов'язані з дитячою порнографією та розповсюдження її за допомогою комп'ютерних систем. Четверта група включає правопорушення, пов'язані з порушенням авторських та суміжних прав [2].

З січня 2013 року під егідою Європолу розпочав діяльність новий Європейський центр боротьби з кіберзлочинністю. Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видах фінансової діяльності, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС [7].

Слід зазначити, що в Україні Департамент по боротьбі з кіберзлочинністю МВС України було створено у грудні 2011 р., а відповідні територіальні підрозділи почали створюватися лише на початку 2012 р. [5].

Проект Незалежної Асоціації банків України «Протидія кіберзлочинності» в банківській сфері стартував у 2013 році та спрямований на взаємодію зацікавлених учасників (банки-члени НАБУ, МВС, НБУ та ін.) у боротьбі з кіберзлочинністю в банківській сфері, а також на інформування клієнтів банків-членів НАБУ про основні правила безпечного використання банківських продуктів і правила поведінки в разі зіткнення з погрозами кібершахрайства.

Концепція Проекту передбачає:

1. Створення на базі Національного банку України Єдиної інформаційної системи обміну інформацією про випадки кібершахрайства (необхідність – запобігання, учасники – банки, НБУ, МВС)

2. Удосконалення нормативно-правових актів, що регулюють питання, які впливають на попередження кіберзлочинності.

3. Підвищення професійного рівня фахівців банків у протидії кіберзлочинності.

4. Підвищення рівня знань населення з метою захисту грошових коштів при розпорядженні своїм розрахунковим рахунком (тема інформування громадян: «Як не стати жертвою кібершахрайства») [4].

У глобальному плані спостерігається широкий діапазон кіберзлочинів, які включають злочини, що здійснюються в цілях отримання фінансової вигоди, злочини, пов'язані з використанням інформації, яка міститься в комп'ютері, а також злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем [7].

Основні види кіберзлочинів узагальнено в табл. 1.

Таблиця 1

Основні види кіберзлочинів у банківській сфері

Вид	Характеристика
Банкоматне шахрайство	- банкоматний скіммінг (виготовлення, збут та встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї); - використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах; - Transaction Reversal Fraud – втручання в роботу банкомату при здійсненні операцій видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником; - Cash Trapping – заклеювання диспенсеру для привласнення зловмисником готівки, яка була списана з карткового рахунку законного держателя картки.
Кіберзлочини в еквайринговій мережі	- укладання фіктивних угод торговельного еквайрінгу для обслуговування підроблених платіжних карток; - викрадення реквізитів платіжних карток, у тому числі із застосуванням технічних засобів їх «клонування»; - операції на суму нижче встановленого ліміту без проведення авторизації; - використання втрачених/викрадених/підроблених платіжних карток.
Шахрайство в системах дистанційного банківського обслуговування (ДБО)	- створення комп'ютерних вірусів та троянських програм для прихованого перехоплення управління комп'ютером клієнта; - відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті несанкціонованих операцій у системах ДБО; - отримання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання у роботу комп'ютерів та систем ДБО клієнтів закордонних банківських установ.
Кіберзлочини в мережі Інтернет	- викрадення реквізитів платіжних карток; - проведення операцій із використанням викрадених реквізитів платіжних карток; - діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток (створення фіктивних WEB-сайтів, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).
Кредитні шахрайства	- отримання кредитів за підробленими документами; - поширення групового шахрайства з залученням у злочинні схеми працівників банків, торгівельних мереж і правоохоронних органів; - налаштування під банківські правила та моделі скорингової оцінки кредитоспроможності позичальників; - фіктивного підтвердження працевлаштування і доходів.

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 встановлення скіммінгових пристроїв на українських банкоматах неодноразово затримувались громадяни Китаю, Румунії, Болгарії та Молдови. В 2013 р. в банкоматах України було виявлено 293 скіммінгові пристрої, що перевищує за-

гальні показники 2012 р. в 4 рази.

За інформацією НБУ України, за 2012 р. загальна кількість шахрайських операцій з платіжними картами в нашій країні зросла відразу на 47% і з 35 до 57 збільшилася кількість банків, з рахунків яких пропали кошти. Як і колись, за кількістю несанкціонованих списань з рахунків лідирували фізичні особи (щодня від населення надходить до 50 скарг, з рахунків за минулий рік пропало 11,4 млн грн). У банківській системі також з'явилися «нововведення»: на зміну скіммінгу, прийшов новий вид крадіжки грошей з банківських карт. Згідно з назвою за даною технологією «Шим» (shim – тонка прокладка), замість тра-диційних громіздких накладок на щілину приймача пластикових карт банкоматів (скімерів), в шиммінгу використовується дуже тонка та гнучка плата, що упроваджується через цю щілину всередину банкомату і практично непомітна. За даними міністерства, в 2011 році було виявлено 45 таких апаратів, у 2012–2013 роках і за перший квартал 2013 року було виявлено вже 37 пристроїв [1].

Для попередження шахрайських схем та мінімізацію збитків клієнтів від банкоматного шахрайства банки встановлюють ліміти на зняття готівки в банкоматах, радять клієнтам періодично змінювати ПІН-код та дотримуватися правил безпеки при використанні банкомату.

В порівнянні з іншими видами шахрайства з платіжними інструментами, кіберзлочинність в еквайринговій мережі України залишається стабільно низькою.

В 2013 р. спостерігалося поступове зниження рівня шахрайства в системах ДБО внаслідок впровадження схеми реагування на інциденти в системах ДБО, що була розроблена спільними зусиллями банків, Держфінмоніторингу, МВС та Асоціації «ЕМА», та допомогла банкам своєчасно виявити та зупинити 90 % спроб несанкціонованих клієнтами переказів [6].

Та все ж, за статистикою в 2013 році зафіксованого 257 спроб несанкціонованого списання коштів з рахунку клієнтів банку на загальну суму 108,75 млн. грн., 7 тис. євро та 115 тис. доларів США.

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 фішингу – 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.

– Крадіжка реквізитів карток з серверів Інтернет-магазинів та створення зловмисниками клонів відомих сайтів, на яких потрібно вводити інфо-

рмацію про платіжну картку.

Доцільно виділити також основні злочинні схеми в мережі Інтернет: купівля-продаж товарів і послуг в Інтернеті шляхом отримання передоплати; створення віртуальних фінансових пірамід в кіберпросторі; прийняття внесків та інвестицій в Інтернет-мережі; розіграш грошових коштів або призів, в тому числі з використанням платних телефонних номерів або коротких повідомлень; озміщення оголошень з пропозиціями прибуткової роботи вдома з обов'язковим вступним внеском; пропозиція перерахувати кошти на так звані «чарівні гаманці», відкриті в небанківських електронних платіжних системах, що нібито автоматично збільшують вкладену суму і повертають її вкладнику.

У 2013 р. слід відзначити тенденцію щодо збільшення випадків кредитного шахрайства. За оцінками служб безпеки українських фінансових установ, рівень загрози від шахрайств по кредитних операціях 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.

Наслідки кіберзлочинності можна розділити на групи: фінансові, юридичні, іміджеві (репутаційні) та технологічні (рис. 1).

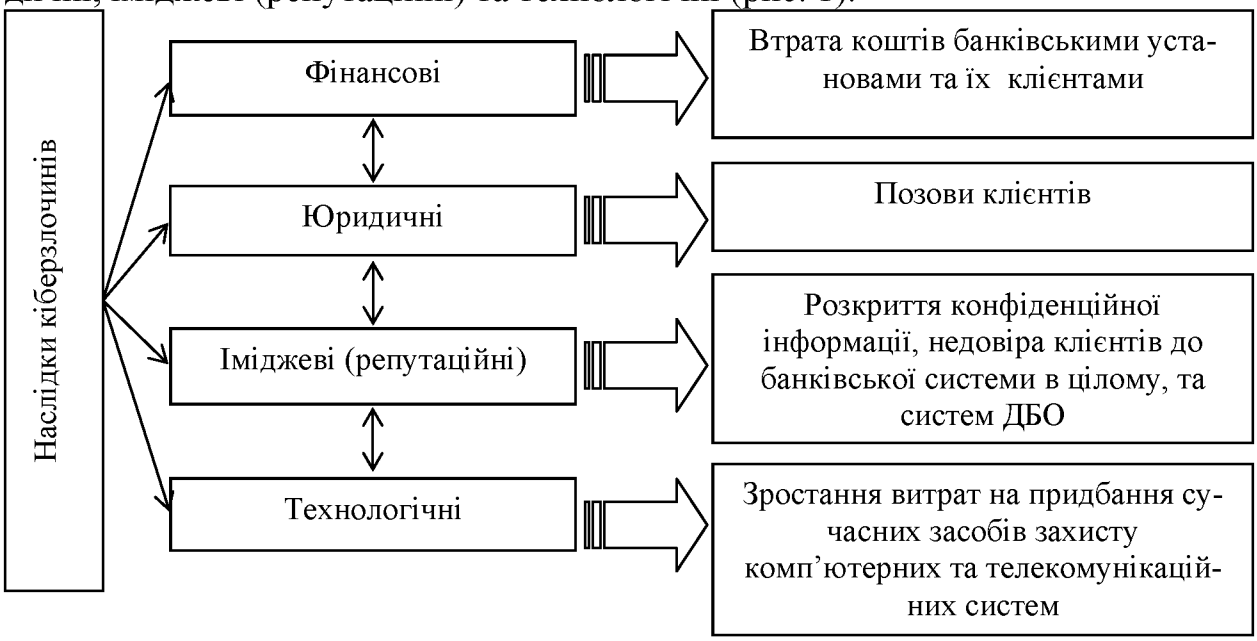

Рис. 1. Наслідки кіберзлочинів

Висновки. Таким чином, питання боротьби з кіберзлочинністю є комплексною проблемою, пріоритетними напрямами вирішення якої можемо виділити:

– удосконалення нормативно-правової бази стосовно протидії кіберзлочинності;

– розробку цілісної державної програми у сфері забезпечення інформаційної безпеки щодо прийняття рішень по виявленню і протидії кіберзлочинам;

– налагодження взаємодії між банківськими установами та правоохоронними органами, спецслужбами, судовою системою;

– забезпечення та удосконалення матеріально-технічної бази, підготовки кваліфікованих фахівців, здатних оперативно виявляти та розслідувати кіберзлочини;

– налагодження механізму ефективної взаємодії правоохоронної системи України з правоохоронними органами закордонних країн, що здійснюють боротьбу з кіберзлочинами.

Список використаних джерел:

1. Голубев В. А. Аналіз кіберзлочинності у сфері економічної безпеки / В. А. Голубев // Information Technology and Security. – 2013. – № 1(3). – С. 26 – 32.

2. Конвенція про кіберзлочинність від 23.11.2001 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/.

3. Кримінальний кодекс України № 2341-III від 05.04.2001. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/.

4. Офіційний сайт Незалежної Асоціації банків України [Електронний ресурс]. – Режим доступу : http ://www.nabu.com.ua/.

5. Правове регулювання кіберзлочинності. [Електронний ресурс] – Режим доступу : http://ukrjustice.com.ua/pravove-rehulyuvannya-kiberzlochynnosti/.

6. Прес-реліз: сучасний стан в сфері кіберзлочинності та кредитного шахрайства в Україні. Рекомендації клієнтам банківських установ. [Електронний ресурс]. – Режим доступу : http://ema.com.ua/press-release-current.

7. Типологічне дослідження «Кіберзлочинність та відмивання коштів». [Електронний ресурс]. – Режим доступу : http://ua.prostobank.ua/spozhivchi_krediti.

Рецензент – к.е.н., професор Аранчій В.І.

УДК 65.018:628.1.033

ЯКІСТЬ ПИТНОЇ ВОДИ ТА ОПТИМІЗАЦІЯ ЇЇ ВИКОРИСТАННЯ

Мироненко О.І., к.с.-г.н., доцент
Полтавська державна аграрна академія

У статті досліджуються питання, щодо якості питної води та раціонального використання водних ресурсів, розглянуто сучасний стан джерел питного водопостачання. У статті також обговорюється значення води для організму людини та аналізується її вміст в організмі людей і тварин.

The article deals with issues concerning drinking water quality and water management, discussed the current state of drinking water sources. The article also discusses the importance of water for the human body and analyze its contents in humans and animals.

Постановка проблеми. Водні ресурси є національним багатством країни, однією з природних основ її економічного розвитку. Вони забезпечують усі сфери життя і господарської діяльності людини, визначають можливості