СЕКЦІЯ 8
ГРОШІ, ФІНАНСИ І КРЕДИТ

УДК: 343.3/.7:343.85:336.71(477)

Бухтіарова А.Г.
кандидат економічних наук,
старший викладач кафедри фінансів, банківської справи та страхування
Сумського державного університету

Гуща А.В.
магістр
Сумського державного університету

Bukhtiarova Alina
PhD in Economics,
Senior Lecturer of the Department of banking, finance and insurance
Sumy State University

Huscha Alina
master student
Sumy State University

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ У БАНКІВСЬКІЙ СФЕРІ

COMBATING CYBERCRIME IN THE BANKING SECTOR

АНОТАЦІЯ

Унаслідок злочинних дій із використанням комп'ютерної техніки банківська система зазнає значних збитків. У статті розкрито сутність поняття «кіберзлочинність», що міститься в законодавчих актах України та міжнародних нормативних документах. Дано характеристику організаційним структурам, які займаються боротьбою з кіберзлочинністю. Досліджено історію виникнення комп'ютерних злочинів. Розкрито специфічні ознаки, що притаманні кіберзлочинності. Досліджено причини підвищення рівня кіберзлочинності в останні десятиліття. Визначено наслідки, що загрожують банківській системі від кіберзлочинів. Розглянуто найбільш поширені комп'ютерні злочини в банківській сфері та підходи до протидії кіберзлочинності, що застосовуються в різних країнах. Визначено запобіжні заходи, до яких удаються вітчизняні банки для протидії кіберзлочинності та мінімізації нанесених збитків банківській установі.

Ключові слова: кіберзлочинність, банки, протидія кіберзлочинності, шахрайство, кібербезпека.

АННОТАЦИЯ

В результате преступных действий с использованием компьютерной техники банковская система несет значительные убытки. В статье раскрыта сущность понятия «киберпреступность», содержащаяся в законодательных актах Украины и международных нормативных документах. Дана характеристика организационным структурам, которые занимаются борьбой с киберпреступностью. Исследована история возникновения компьютерных преступлений. Раскрыты специфические признаки, присущие киберпреступности. Исследованы причины повышения уровня киберпреступности в последние десятилетия. Определены последствия киберпреступлений, угрожающие банковской системе. Рассмотрены наиболее распространенные компьютерные преступления в банковской сфере и подходы к противодействию киберпреступности, применяемые в различных странах. Определены меры, к которым прибегают отечественные банки для противодействия киберпреступности и минимизации нанесенного ущерба банковским учреждениям.

Ключевые слова: киберпреступность, банки, противодействие киберпреступности, мошенничество, кибербезопасность.

ANNOTATION

Nowadays there is a rapid spread of cybercrime, which, at the same time, is becoming increasingly difficult to investigate. As a result of criminal activities involving the use of computer technology and banking system suffers heavy losses. A comprehensive analysis of cybercrime and methods of combating it is needed to find ways to overcome this problem. The article reveals the essence of the concept of "cybercrime", which is contained in the legislative acts of Ukraine and international normative documents. A description of the organizational structures involved in the fight against cybercrime is given. The history of the occurrence of computer crimes in the world and the process of their spread on the territory of Ukraine is researched. The specific features of cybercrime as a kind of economic crimes are revealed. The reasons of increase of level of cybercrime in the last decades are investigated. The consequences, which threaten the banking system from the illegal activity of cybercriminals, namely: financial, image (reputation), legal, technological, are determined. The most widespread crimes in the banking sphere, which are caused by the use of computer technology, including ATM fraud, fraud in trade and service networks, the Internet, in remote banking services, are considered. The role and functions of the National Bank of Ukraine and other government agencies in combating cybercrime in the banking system are determined. Authors analyze the level of disclosure of criminal cases in the investigation of cybercrime in Ukraine and the responsibility of convicted persons for the criminal offenses committed. Banking sector's protection systems in Ukraine have a low level of development. Therefore, it is expedient to analyze the experience of foreign countries. The article deals with approaches to counteracting cybercrime, which are used in China, USA, Poland, Australia, Belgium, Belarus, etc. The preventive measures taken by domestic banks for the purpose of counteracting cybercrime and minimization of losses incurred by the banking institution and persons it represents are determined.

Key words: cybercrime, banks, combating cybercrime, fraud, cybersecurity.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Щоденна робота урядових структур, банківської, енергетичної, транспортної та інших систем неможлива без використання комп'ютерної техніки, мереж зв'язку та інших технічних засобів. Але водночас інформаційний простір став місцем і безпосередньо інструментом злочину.

Поява кіберзлочинності пов'язана з виникненням так званого віртуального простору, який містить інформацію про осіб, події, явища, процеси тощо, зашифровані у математичному, символьному чи будь-якому іншому вигляді

Рівень кіберзлочинності в Україні в останні десятиліття був мінімальним, оскільки розвиток інформаційних технологій перебував на нижчому рівні, ніж у розвинених країнах світу.

Швидкий розвиток інформаційного суспільства дав поштовх до поширення кіберзлочинів, які все частіше скоюються на території України та з кожним роком набувають усе ширших масштабів.

Існують й інші передумови підвищення зацікавленості злочинців кіберпростором: відсутність фізичного контакту з жертвою або представниками фінансової установи, оперативність здійснення, анонімність, доступність комп'ютерної техніки, віддаленість об'єкта злочинних посягань. Інтернет-простір – це не лише місце скоєння злочину, а й місце легалізації незаконно отриманих доходів. Різноманітні види кіберзлочинів у поєднанні зі способами відмивання доходів призводять до ускладнення їх розслідування.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спираються автори. Питання боротьби з кіберзлочинністю були предметом досліджень багатьох учених. Цій проблематиці в різні часи приділяли увагу такі фахівці, як О.В. Орлов, Ю.М. Онищенко [1], П.І. Пушкаренко [6], В.О. Голубєв [7], М.В. Гуцалюк [8], Є.В. Зозуля [11], Ю.М. Барташевська [12], М.І. Доусчі [13]. Незважаючи на досить велику кількість праць, питання запобігання поширенню кіберзлочинності у банківському секторі залишається актуальним, а постійне вдосконалення кібертехнологій вимагає розроблення нових методів боротьбі із шахрайством у цій сфері.

Формулювання цілей статті **(постановка завдання).** Метою статті є дослідження проблеми кіберзлочинності в Україні, зокрема в банківській сфері, та оцінка ефективності наявних методів боротьби з комп'ютерними злочинами.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Дослідженню сутності кіберзлочинності приділялося чимало уваги, проте в наукових та правових колах відсутній єдиний підхід до його трактування. Експертами Управління ООН із наркотиків і злочинності зазначається, що визначення кіберзлочинності, головним чином, залежить від того, в яких цілях цей термін буде використовуватися. Основою кіберзлочинності є обмежене число діянь, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних даних чи систем.

Згідно з рекомендаціями експертів ООН, термін «кіберзлочинність» охоплює будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи або мережі, у рамках комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі [1, с. 4].

Поняття кіберзлочинності безпосередньо не розкрито нормами Конвенції «Про кіберзлочинність» від 23.11.2001, яку було ратифіковано Україною у 2005 р. [2]. Але все ж у цьому міжнародному документі містяться вказівки на: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані з порушенням авторських та суміжних прав.

У Конституції України поняття «боротьба із кіберзлочинністю» відсутнє, але у ст. 17 Конституції зазначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави та справою всього Українського народу [3]. В Україні як кіберзлочини кримінальним законом передбачено і закріплено в окремому Розділі XVI Кримінального кодексу України суспільно небезпечні діяння «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [4].

Таким чином, поняття «кіберзлочин» було відсутнє в українському законодавстві до моменту прийняття Закону України «Про основні засади забезпечення кібербезпеки України» у 2017 р.: «Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [5].

У цьому Законі визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки.

Таким чином, до нормативно-правових актів, які становлять нормативно-правову базу боротьби з комп'ютерними злочинами в Україні, слід віднести: Конституцію України, Кримінальний кодекс України, Конвенцію про кіберзлочинність, закони України «Про інформацію» № 2657-XII від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994, «Про державну таємницю» № 3855-XII від 21.01.1994, «Про основи національної безпеки України» № 964-IV від 19.06.2003, «Про осно-

вні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.

Для протидії кіберзлочинності в Україні створено спеціальні організаційні структури, а саме: Урядову комісію з питань інформаційно-аналітичного забезпечення органів виконавчої влади, Міжвідомчий комітет із проблем захисту прав на об'єкти інтелектуальної власності, Міжвідомчу робочу групу з розроблення та узгодження Концепції легалізації програмних продуктів та боротьби з їх нелегальним використанням.

У 2011 р. було відкрито Департамент з боротьби із кіберзлочинністю МВС України, а відповідні територіальні підрозділи почали створюватися на початку 2012 р.

5 листопада 2015 р. була створена нова Кіберполіція як структурний підрозділ Національної поліції. Основною метою створення кіберполіції було реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

На початку 2016 р. Незалежна асоціація банків України (НАБУ) запустила проект «Протидія кіберзлочинності», покликаний підвищити обізнаність клієнтів банків про безпечну поведінку. Партнерами проекту виступили НБУ, МВС та 19 комерційних банків.

В Україні на базі НЦБ Інтерполу створено Національний центральний консультативний пункт із проблем комп'ютерної злочинності. Це надало можливості накопичити матеріал про законодавче регулювання та організаційний досвід боротьби з кіберзлочинністю в різних країнах.

Щодо банківської сфери, то в структурі НБУ є окремий структурний підрозділ – Департамент безпеки, однією з основних функцій якого є розроблення та реалізація стратегії і політики інформаційної безпеки НБУ, впровадження новітніх технологій із метою захисту інформації в інформаційній інфраструктурі банківської системи України.

Хоча правова та організаційна структура протидії кіберзлочинності в Україні активно почала формуватися в останні кілька років, цей вид злочину не є новим для суспільства.

Вчинення першого в історії комп'ютерного злочину відбулося у Міннесоті, де в 1966 р. зафіксовано перший випадок використання електронної обчислювальної машини як інструмента під час пограбування банку. Саме у цей період виник термін «комп'ютерна злочинність» [6, с. 79].

На територію колишнього СРСР, до складу якого входила й Україна, кіберзлочини поширилися у 1979 році, коли у Вільнюсі внаслідок кіберзлочину була нанесена шкода державі в розмірі 80 тисяч карбованців. Тобто різниця у розвитку комп'ютерної злочинності у світових державах та у Радянському Союзі становила понад десять років.

Наступна важлива подія в історії розвитку кіберзлочинності – так звана «справа Володимира Льовіна», учасника організованої злочинної групи, яка, використовуючи Інтернет, у 1994 р. викрала понад 12 млн дол., які належали корпоративним клієнтам американського «Сітібанку». Ця справа вважається першою, віднесеною до категорії транснаціональних мережевих комп'ютерних злочинів [7, с. 6].

Державні органи технологічно розвинутих країн усвідомили, наскільки серйозними наслідками може обернутися для інформаційного світу комп'ютерна злочинність у разі відсутності відповідного реагування на неї, тому у структурі поліцій світу почали з'являтися спеціальні підрозділи з боротьби із цим видом злочинності.

У березні 2018 р. в Іспанії був заарештований лідер організованого злочинного угруповання,

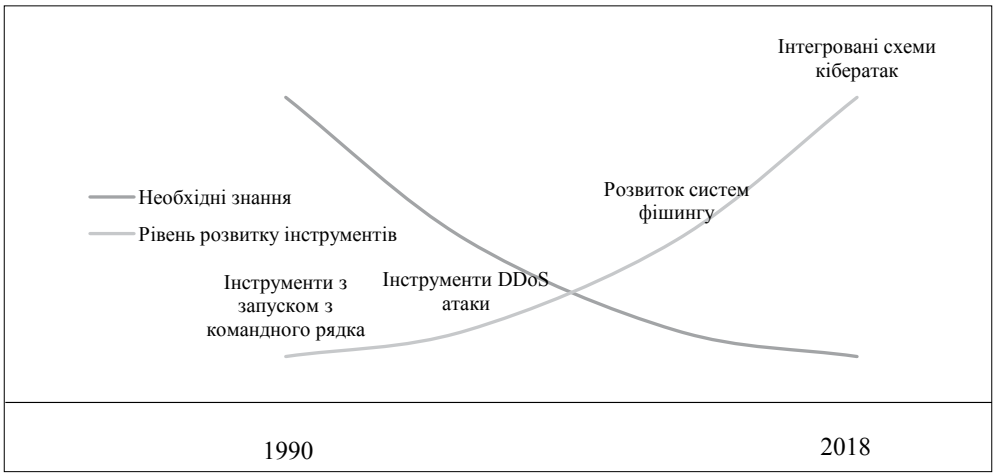

Рис. 1. Співвідношення рівня розвитку інструментів кіберзлочинців та рівня технічних знань [9, с. 24]

який виявився 34-річним українцем. Це угруповання з 2013 р. здійснювало кібератаки на банки, системи електронних платежів та фінансові установи, використовуючи свої власні розробки. Понад 100 банків із 40 країн світу постраждало в результаті діяльності злочинців, а викрадена сума перевищувала 1 млрд євро [8, с. 123].

Із кожним роком зі зростанням рівня розвитку інструментів кіберзлочинність вимагає все менше технічних знань (рис. 1).

Експерти зазначають, що саме хакери в недалекому майбутньому змістять тероризм і стануть загрозою номер один для країн, адже, незважаючи на те що злочини відбуваються у віртуальному світі, збиток вони завдають реальний. «Небезпека з боку Інтернет-злочинності є більш серйозною, ніж із боку ядерної зброї», – заявляє голова Комісії внутрішніх справ Парламенту Великобританії, депутат Кіт Ваз [10, с. 82].

Наведені приклади свідчать, що саме 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].

Щодо України, то кіберзлочини є п'ятим за розміром видом економічної злочинності після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю (рис. 2).

Рис. 2. Найпоширеніші економічні злочини в Україні та світі [13, с. 21]

Незважаючи на значну кількість виявлених кіберзлочинів в Україні, кількість засуджених осіб є незначною: 70 у 2018 р. проти 42 у 2017 р. Протягом цих років лише по дві особи були позбавлені волі на строк до п'яти років. Тобто часто покарання за вчинення кіберзлочинів обмежується лише невеликим штрафом, тому що ці злочини кваліфікуються як злочини середньої тяжкості.

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.

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

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 кіберзлочинності 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.

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);

2) 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);

3) 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);

4) 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) [14, с. 11].

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. 3) [15].

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 охоронюваної законом банківської таємниці.

Наслідком значної кількості кіберзлочинів у вказаній сфері є зниження довіри громадян у цілому до надійності фінансової системи, інституту банківської таємниці, надійності захисту персональних даних, а також до фінансових операцій, що проводяться з використанням новітніх технологій.

При цьому недовіра населення до ринків фінансових послуг не дає можливості активно використовувати вільні кошти громадян як інвестиційні ресурси, що спрямовуються на розвиток економіки.

У цілому такі наслідки можливо розділити на такі групи: фінансові, іміджеві (репутаційні), юридичні, технологічні (рис. 4).

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

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.

Наприклад, у Китаї 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.

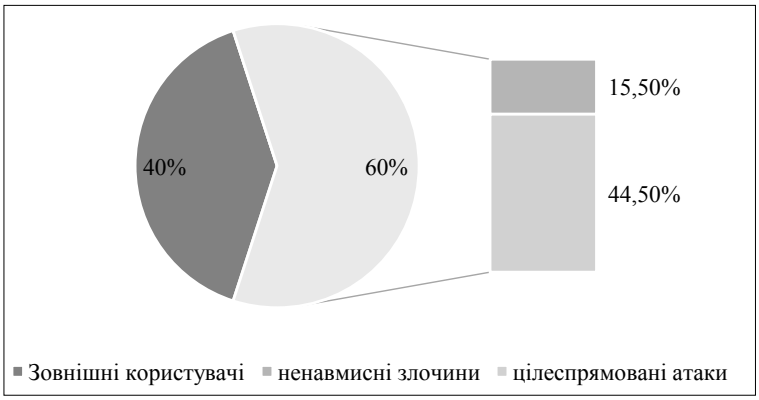

Рис. 3. Особи, які несуть відповідальність за кібератаки

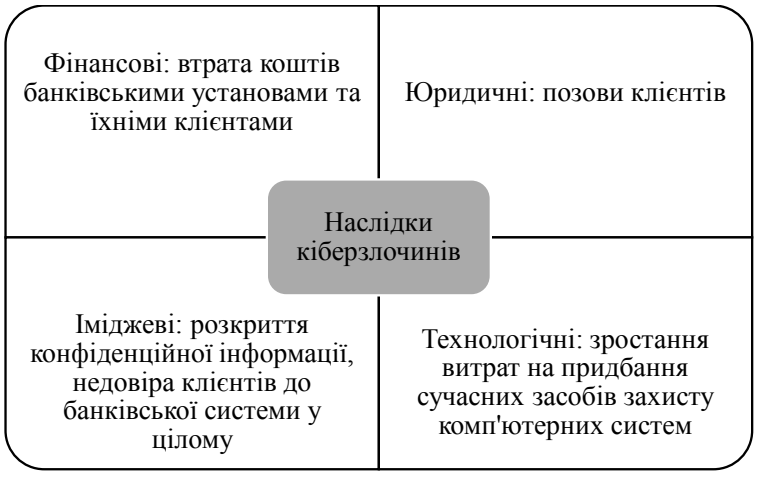

Рис. 4. Наслідки кіберзлочинів

У зв'язку з наростанням сум, утрачених клієнтами, в Україні дана проблема також потребує врегулювання на законодавчому рівні, тому що зараз постраждалі клієнти самостійно через судові позови намагаються повернути втрачені кошти, і у кожному разі існує проблема з доказуванням провини сторін [16].

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, Швейцарії, Швеції та ін. Серед основних функцій цих підрозділів виділяють:

– моніторинг кіберпростору з метою виявлення кіберзлочинів;

– здійснення оперативно-розшукових та розвідувальних заходів для фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів, надання методичної та практичної допомоги іншим органам, зокрема правоохоронним, у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактика кіберзлочинів за допомогою громадськості та засобів масової інформації.

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.

Протидія кіберзлочинам поєднує комплекс правових, технічних, організаційних та інформаційних заходів, де роль кожного із цих заходів не може бути визначена як пріоритетна чи другорядна. При цьому ефективна протидія відмиванню злочинних доходів та зниження рівня злочинності у цій сфері можливі завдяки своєчасному виявленню фінансових операцій, що можуть бути пов'язані з відмиванням доходів від кіберзлочинності, та ефективному співробітництву між державним та приватним секторами.

Слід зазначити, що значна частина кіберзлочинів стає можливою через необізнаність населення та недотримання ним основних правил безпеки, тому значну користь у попередженні кіберзлочинності мають інформаційно-просвітницькі заходи щодо нових ризиків та загроз в інформаційних та комп'ютерних системах.

Для протидії кіберзлочинності та мінімізації нанесених збитків банківській установі та особам, яких вона представляє, банки вдаються до таких запобіжних заходів:

– ретельно перевіряють спеціалістів під час прийому на роботу;

– для захисту інформації вибирають сучасні інформаційні системи;

– користуються послугами кваліфікованих комп'ютерних спеціалістів;

– займаються розробленням власних антихакерських програм;

– створюють та постійно поповнюють власні бази даних осіб, що були причетними до скоєних кіберзлочинів;

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

Висновки з цього дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, сьогодні в Україні створено умови для боротьби з кіберзлочинністю, визначено основні цілі, напрями та принципи державної політики. Але існують питання у сфері кібербезпеки, які потребують оперативного вирішення.

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. 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.

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.

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.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. 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.

2. Конвенція про кіберзлочинність. *Офіційний вісник України.* 2007. № 65. С. 107.
3. Конституція України від 26.06.1996 № 254к/96-ВР (ред. від 07.02.2019). *Відомості Верховної Ради.* 1996. № 30. Ст. 141.
4. Кримінальний кодекс України від 05.01.2001 (ред. від 19.05.2019). *Відомості Верховної Ради*. 2001. № 25–26. Ст. 131.
5. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
6. Пушкаренко П.І. Кіберзлочинність як новітній феномен тіньової економіки. *Проблеми і перспективи розвитку банківської системи України*. 2006. Т. 17. С. 75–82.
7. Голубів В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навчальний посібник / за заг. ред. д.ю.н., проф. Р.А. Калюжного. Запоріжжя : ГУ «ЗІДМУ». 2002. 292 с.
8. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1. С. 118–128.
9. Гайдош Т. Киберпреступность преобретает индустриальный характер. *Финансы и развитие*. 2018. № 2. С. 22–27.
10. Безпека підприємництва : інформаційний бюлетень. Київ : Український союз промисловців і підприємців, 2013. № 6. 97 с.
11. Зозуля Є.В. Діяльність органів державної влади та управління України щодо нормативно-правового та організаційного забезпечення міжнародного співробітництва у боротьбі з кіберзлочинністю. *Право і суспільство*. 2011. № 4. С. 80–85.
12. Барташевська Ю.М. Оцінка ефективності витрат компанії на інформаційну безпеку. *Науковий вісник Міжнародного гуманітарного університету*. 2017. № 27. С. 87–90.
13. 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.
14. Кіберзлочинність та відмивання коштів. Київ : Державна служба фінансового моніторингу України. 2013. 53 с. URL: http://www.sdfm.gov.ua/ content/file/Site_docs/2013/20131230/tipolog2013.pdf (дата звернення: 11.06.2019).
15. IBM Cyber Security Intelligence Index 2016. 2016. 156 p. URL: https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2015.pdf (дата звернення: 11.06.2019).
16. Here's another reason to think twice before using your debit card. *CNBC* : вебсайт. URL: https://www.cnbc.com/2018/03/06/protect-your-bank-accounts-from-rising-debit-card-fraud.html (дата звернення: 11.06.2019).

REFERENCES:

1. Orlov O. V. (2013) Aktualni napriamy derzhavnoi polityky Ukrainy u sferi borotby z kiberzlochynnistiu [Current trends of the state policy of Ukraine in the field of combating cybercrime]. *Teoriia ta praktyka derzhavnoho upravlinnia*, no 3, pp. 3–9.
2. Convention on Cybercrime (2007, September 10). *Ofitsiinyi visnyk Ukrainy* Konventsiia pro kiberzlochynnist, 65, 107.
3. Constitution of Ukraine. (1996, June 26). *Vidomosti Verkhovnoi Rady*. Kyiv: Parlam. vyd-vo [in Ukrainian].
4. The Crimean Code of Ukraine. (2001, January 1). *Vidomosti Verkhovnoi Rady Ukrayiny*. Kyiv: Parlam. vyd-vo [in Ukrainian].
5. Law of Ukraine on the basic principles of providing cyber security of Ukraine № 2163-VIII. (2017, November 5). *Vidomosti Verkhovnoi Rady Ukrayiny,* 45, 403 [in Ukrainian].
6. Pushkarenko P. I. (2006) Kiberzlochynnist yak novitnii fenomen tinovoi ekonomiky [Cybercrime as the latest phenomenon of the shadow economy]. *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy : zbirnyk naukovykh prats*, vol. 17, pp. 75–82.
7. Holubiv V. O., Havlovskyi V. D., Tsymbaliuk V. S. (2002) *Problemy borotby zi zlochynamy u sferi vykorystannia kompiuternykh tekhnolohii* [Problems in combating crime in the field of computer technology use]. Zaporizhzhia: HU "ZIDMU". (in Ukrainian).
8. Hutsaliuk M. V. (2019) Suchasni tendentsii orhanizovanoi kiberzlochynnosti [Modern trends in organized cybercrime]. *Informatsiia i parvo,* no 1, pp. 118–128.
9. Gaydosh T. (2018) Kiberprestupnost' preobretaet industrial'nyy kharakter [Cybercrime gains industrial character]. *Finansy i razvitie*, no 2, pp. 22–27.
10. Ukrainskyi soiuz promyslovtsiv i pidpryiemtsiv (2013) *Bezpeka pidpryiemnytstva* [Business security], Kyiv : Ukrainskyi soiuz promyslovtsiv i pidpryiemtsiv.
11. Zozulia Ye. V. (2011) Diialnist orhaniv derzhavnoi vlady ta upravlinnia Ukrainy shchodo normatyvno-pravovoho ta orhanizatsiinoho zabezpechennia mizhnarodnoho spivrobitnytstva u borotbi z kiberzlochynnistiu [Activities of state authorities and management of Ukraine on normative and legal and organizational support of international cooperation in the fight against cybercrime]. *Pravo i suspilstvo*, no 4, pp. 80–85.
12. Bartashevska Yu. M. (2017) Otsinka efektyvnosti vytrat kompanii na informatsiinu bezpeku [Estimation of efficiency of company expenses on information security]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu*, no 27, pp. 87–90.
13. Douschi M. I. (2018) Pravove rehuliuvannia zabezpechennia kiberbezpeky v Ukraini [Legal regulation of cyber security in Ukraine]. Proceedings of the *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia Proceedings of the Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia* (Ukraine, Odesa, November 30), Odesa : ODUVS, pp. 21–23.
14. Derzhavna sluzhba finansovoho monitorynhu Ukrainy (2013) Kiberzlochynnist ta vidmyvannia koshtiv [Cybercrime and money laundering], available at http://www.sdfm.gov.ua/content/file/site_docs/2013/20131230/tipolog2013.
15. IBM Cyber Security Intelligence Index (2016), available at https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2015.pdf.
16. CNBC (2018) Here's another reason to think twice before using your debit card, available at https://www.cnbc.com/2018/03/06/protect-your-bank-accounts-from-rising-debit-card-fraud.html.