УДК 347.738
DOI https://doi.org/10.32782/2524-0374/2021-3/58

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У БАНКІВСЬКІЙ СФЕРІ

LEGAL BASIS OF CYBER SECURITY IN THE BANKING SPHERE

Тімашов В.О., д.ю.н., доцент,
професор кафедри адміністративного, фінансового та інформаційного права
Київський національний торговельно-економічний університет

Корольова О.А., студентка ІІІ курсу
факультету міжнародної торгівлі та права
Київський національний торговельно-економічний університет

Юрченко Д.Г., студент ІІІ курсу
факультету міжнародної торгівлі та права
Київський національний торговельно-економічний університет

У наш час відбувається швидке поширення кіберзлочинності, яку водночас стає все важче розслідувати. У результаті злочинної діяльності, пов'язаної з використанням комп'ютерних технологій, банківська система зазнає значних втрат. Для пошуку шляхів подолання цієї проблеми необхідний всебічний аналіз кіберзлочинності та методів боротьби з нею.

Стаття розкриває суть поняття кіберзлочинності, яке міститься в законодавчих актах України. Розкрито особливості кіберзлочинності як виду економічного злочину, його транскордонну природу та фактори затримки. Розглянуто думки низки науковців щодо проблем кібербезпеки. Досліджено причини підвищення рівня кіберзлочинності. Визначено наслідки, які загрожують банківській системі від незаконної діяльності кіберзлочинців, а саме: фінансові, іміджеві (репутаційні), юридичні, технологічні. Розглядаються найпоширеніші злочини в банківській сфері, які спричинені використанням комп'ютерних технологій, включаючи шахрайство з банкоматами, шахрайство у послугах віддаленого банку.

Досліджено способи боротьби з кіберзлочинністю і методи упередження таких злочинів та їхня ефективність. Зроблено аналіз практики розслідування кіберзлочинів у банківському секторі. Розглянуто методи вчинення кіберзлочинності, включаючи: перехоплення паролів користувачів, використання програмних помилок, використання помилок механізмів ідентифікації користувачів, використання недоліків протоколів передачі даних, отримання інформації про користувачів за допомогою стандартних операційних систем та інші види злочинів.

Проаналізовано профілактичні заходи, що здійснюються вітчизняними банками з метою протидії кіберзлочинності та мінімізації збитків, понесених банківською установою. Також досліджено досвід провідних країн світу щодо запобігання кіберзлочинності. Розглянуто міжнародне співробітництво в сфері захисту інформації та рейтинг кібербезпеки серед країн світу. Порівняно думки експертів в сфері кібербезпеки щодо майбутнього кіберзлочинів та їх еволюції в найближчий час.

Зроблено висновок щодо неможливості повного захисту від кібератак через невпинний розвиток інформаційних технологій. Названі підстави, що сприяють розвитку кіберзлочинності в сучасному світі. Визначено негативні фактори, через які відбувається зниження ефективності боротьби з кіберзлочинністю в Україні. Зазначено, що створення системи навчання в галузі кібербезпеки в банках, моніторинг кіберпростору для своєчасного запобігання кіберзагрозам позитивно відобразиться на статистиці злочинності в інформаційній сфері. Зроблені рекомендації щодо змін у законодавстві, дотримання мінімальних правил безпеки мережі та впровадження нових заходів кібербезпеки у банківській сфері з метою забезпечення охорони та захисту інформації як банків, так і їхніх клієнтів.

Ключові слова: кіберзлочинність, банківська система, електронний банкінг, правопорушення, інтернет-шахрайство.

Nowadays, cybercrime is spreading rapidly, and at the same time it is becoming increasingly difficult to investigate. As a result of criminal activities related to the use of computer technology, the banking system suffers significant losses. To find ways to overcome this problem, a comprehensive analysis of cybercrime and methods to combat it is needed.

The article reveals the essence of the concept of "cybercrime", which is contained in the legislation of Ukraine. The peculiarities of cybercrime as a type of economic crime, its cross-border nature and delay factors are revealed. The opinions of a number of scientists on cybersecurity issues are considered. The reasons for the increase in the level of cybercrime have been studied. The consequences that threaten the banking system from the illegal activities of cybercriminals have been identified, namely: financial, image (reputational), legal, technological. The most common crimes in the banking sector, which are caused by the use of computer technology, including fraud with ATMs, fraud in the services of a remote bank.

Methods of combating cybercrime and methods of preventing such crimes and their effectiveness are studied. An analysis of the practice of investigating cybercrime in the banking sector is made. Methods of committing cybercrime are considered, including: interception of user passwords, use of software errors, use of errors of user identification mechanisms, use of shortcomings of data transmission protocols, obtaining information about users using standard operating systems and other types of crimes.

Preventive measures taken by domestic banks to combat cybercrime and minimize losses incurred by the banking institution and the persons it represents are analyzed. The experience of the world's leading countries in preventing cybercrime is also studied. International cooperation in the field of information protection and cybersecurity rating among the countries of the world are considered. The opinions of cybersecurity experts on the future of cybercrime and their evolution in the near future are compared.

It is concluded that it is impossible to fully protect against cyberattacks due to the constant development of information technology. The bases promoting development of cybercrime in the modern world are named. The negative factors that reduce the effectiveness of the fight against cybercrime in Ukraine have been identified. It is noted that the creation of a training system in the field of cybersecurity in banks; cyberspace monitoring for the timely prevention of cyber threats will have a positive impact on crime statistics in the information sphere. Recommendations were made on changes in legislation, compliance with minimum network security rules, and the introduction of new cybersecurity measures in the banking sector to ensure the protection and security of information of both banks and their customers.

Key words: cybercrime, banking system, electronic banking, delinquency, internet fraud.

Постановка проблеми. Зі зростанням кількості користувачів Інтернету зростають такі фактори ризику, як: залежність суспільства від інформаційних технологій, а потім вразливість до різного роду посягань на інформацію; також зростає можливість використання мережі для вчинення злочинів та можливість стати жертвою використання інформаційних технологій у злочинних цілях. Водночас вчинення злочину не вимагає великих зусиль і витрат – досить мати комп'ютер, програмне забезпечення та зв'язок з інформаційною мережею. Вам навіть не потрібно мати глибоких технічних знань: існують спеціальні форуми, на яких ви можете придбати програмне забезпечення для скоєння злочинів, викрадені номери кредитних карток та облікові дані користувачів, а також

скористатися послугами, які допоможуть вам здійснити електронні розкрадання та атаки на комп'ютерні системи.

В Україні та в усьому світі щороку здійснюються десятки тисяч злочинів із використанням інформаційно-комунікаційних технологій, програмного, програмно-технічного забезпечення, інших технічних та технологічних засобів та обладнання. Щодня людей та компанії позбавляють персональних даних, коштів із рахунків, збирають конфіденційну та комерційну інформацію, блокують діяльність тощо. Однак успіх попередження таких злочинів, їх викриття та притягнення винних до відповідальності нині є досить рідкісним явищем порівняно з кількістю таких правопорушень. Це не дивно, адже кіберпростір безмежний, а досвідчені хакери мають усі необхідні навички та інструменти, щоб залишатись анонімними. Сьогодні кібератаки завдають шкоди не лише фізичним та юридичним особам, а й державі. Щороку у всьому світі проводяться сотні заходів різного рівня для обговорення актуальних проблем кібербезпеки. У літературних словниках постійно з'являються нові визначення: кіберінтелект, кібертероризм, кібершпигунство, кіберпростір тощо. Кібербезпека та боротьба з кіберзлочинністю у XXI столітті є одними з найважливіших питань, що вимагають глибокого аналізу, розроблення та впровадження високотехнологічних рішень для запобігання та виявлення кіберзагроз. Ось чому захист інформаційної безпеки є пріоритетом як для країни загалом, так і для спеціально уповноважених відомств зокрема.

Аналіз останніх досліджень і публікацій. Проблема кібербезпеки є темою розгляду низки науковців, таких як: В.М. Бутузов, А.Г. Бухтярова, А.В. Гуща, В.Є. Козлов, М. Кравцова, Н.В. Лута, Н.В. Зачосовна, М. Кацера, С. Федушко, Є. Бєнова та інші.

Мета статті. Головною метою цієї роботи є аналіз та систематизація теоретичного досвіду та практичних заходів щодо боротьби з кіберзлочинністю в банківському секторі з метою виявлення перспективних шляхів боротьби зі злочинами в кіберпросторі України.

Виклад основного матеріалу дослідження. У сучасних умовах актуальною проблемою як банків, так і їхніх клієнтів є загроза використання інформаційних технологій у злочинних цілях, відома як кіберзлочинність. Це один із найпоширеніших видів економічної злочинності в сучасній Україні. Кіберзлочинність вважається соціально небезпечним діянням, що здійснюється із застосуванням сучасних технологій та комп'ютерної техніки з метою заподіяння шкоди майну або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадських організацій та громадян.

Злочинна діяльність, яка щороку набуває нових форм, методів і технологій вчинення злочинів, є невід'ємною частиною суспільного життя. Віртуальні злочини набувають широкого поширення у банківському секторі. Кількість злочинів, скоєних шляхом отримання доступу до кодів банківських карток та незаконного вилучення коштів із рахунків, щороку зростає. Поширення віртуальних форм злочинності пов'язане насамперед із швидким розвитком технологій, підвищенням ролі інформації у суспільному житті та можливістю здійснювати злочини віддалено. Кіберзлочинність особливо приваблива завдяки здатності приховувати або знищувати його сліди, відсутності фізичного контакту з жертвою чи фінансовою установою, оперативності, анонімності, наявності комп'ютерного обладнання, віддаленості об'єкта злочинного посягання тощо.

Діяльність боротьби з кіберзлочинністю посідає особливе місце у діяльності правоохоронних органів через прихований характер таких правопорушень та постійне оновлення механізму їх вчинення. Процес розслідування цих злочинів ускладнюється труднощами виявлення та фіксації слідів злочинів у віртуальному просторі. Питання розслідування віртуальних злочинів у банківському секторі викликане специфікою їх вчинення, що вимагає спеціальних знань правоохоронців. Також варто зазначити, що кіберзлочинність є міжнародною за своєю суттю, тому існує необхідність співробітників правоохоронних органів співпрацювати на міжнародному рівні, щоб мінімізувати рівень віртуальних злочинів у банківському секторі. Ця ситуація визначає значення теоретичного дослідження процесу розслідування кіберзлочинності банківського сектору з метою розроблення заходів, що сприяють підвищенню кібербезпеки як на національному, так і на міжнародному рівні.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого у 2017 році, визначено поняття кіберзлочину (комп'ютерний злочин) – це 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 (п. 8 ст. 1), також згідно з п. 9. ст. 1 кіберзлочинність визначається як сукупність кіберзлочинів [1].

Згідно з дослідженням, проведеним PwC у 2018 році, 31% організацій в Україні постраждали від кіберзлочинності. Більше третини українських організацій, які постраждали від кібератак, постраждали від зловмисного програмного забезпечення. У результаті кібератак були не тільки порушені бізнес-процеси організацій, але й завдані значні втрати організаціям [2].

Слід зазначити, що в банківському секторі здійснюється набагато більше кіберзлочинів, ніж офіційно повідомляється. А.Г. Бухтіарова та А.В. Гуща зазначають, що причиною є те, що багато кібератак не є успішними, а виявлені прогалини в системі електронного банкінгу швидко відновлюються. Поширення інформації про спроби кібершахрайства може вплинути на рівень довіри клієнтів до банківської установи. Як результат, клієнти банку можуть почати масово вилучати свої банківські депозити з банків, що створить серйозну проблему для банків через різке збільшення ризику ліквідності, тому складно оцінити справжній рівень кіберзлочинності [3, с. 358].

Хочемо зазначити, що саме хакери найближчим часом витіснять тероризм і стануть загрозою номер один для країн, оскільки, незважаючи на те, що злочини відбуваються у віртуальному світі, вони завдають реальної шкоди. Саме фінансовий сектор економіки, включаючи банки та їхні послуги, вважається найбільш привабливим для кіберзлочинців, а фінансові дані є однією з найпопулярніших цілей кібератак, оскільки їх використання дозволяє злочинцям заробляти значні гроші. За даними Інтерполу, прибуток від кіберзлочинності в банківському секторі посідає третє місце у світі після надходжень від незаконного обігу наркотиків та незаконного обігу зброї [3, с. 358].

Ю. Когут вважає, що крадіжка грошей просто з банківських рахунків або використання викрадених персональних даних – не єдиний мотив злому систем безпеки. Такі кібератаки часто можуть бути спрямовані на підрив репутації фінансової установи. DDoS-атаки також використовуються для відволікання служб безпеки банку від шахрайських схем та злому рахунків. Напади часто здійснюються на веб-сайти великих банків, які не мають належного захисту. На думку експертів, нині чотири з п'яти банківських ресурсів є вразливими, а три з чотирьох атак здійснюються через незахищені програми, і одна невелика уразливість може становити загрозу для всієї фінансової установи [4, с. 58].

Традиційною темою кіберзлочинності є банківська картка. Основними видами кіберзлочинів у цій сфері є:

− Скіммінг – вид кіберзлочинності, скоєний пристроєм для зчитування інформації з пластикових карток. Станом на 2013 рік у банкоматах України було виявлено 293 скіммінг-пристроїв. За словами представника

Департаменту кіберполіції Національної поліції України Віталія Новіка, в 2019 році в українських банкоматах було виявлено 100 скіммінг-пристроїв, а за 50 фактами порушено 14 кримінальних справ [5].

– Шахрайство в системах віддаленого банку – це різновид кіберзлочинності, в результаті якого злочинці можуть відстевувати будь-які банківські операції [6, с. 103].

Крім того, у банківському секторі існують такі типи кіберзлочинності:

1. Фішинг як вид інтернет-шахрайства, за допомогою якого злочинцям вдається отримати дані клієнтів банку: викрадення паролів, номерів, даних кредитних карток, банківських рахунків та іншої конфіденційної інформації.

2. Вішинг – вид шахрайства за допомогою мобільного телефону. Шахраї телефонують на певний номер, і абонент повідомляє конфіденційні дані на банківських рахунках.

3. Фітинг – дублікат сайту як дзеркало реального сайту. Під час онлайн-покупки за допомогою банківської картки клієнт вводить свої дані, і в цей час зловмисники знімають з неї кошти. Запобігти входу на такий сайт можна, якщо дотримуватися таких заходів: ввести адресу сайту вручну; не відвідувати рекламні сайти; перевіряти, чи цей сайт має безпечне з'єднання [6, с. 104].

Також класифікують кіберзлочини за методами втручання в процес передачі даних:

– переривання (блокування процесу передачі);

– перехоплення (незаконний доступ до переданих даних);

– модифікація (незаконна зміна даних);

– виробництво (організація фальсифікованого сеансу спілкування).

Також методи вчинення кіберзлочинності включають: перехоплення паролів інших користувачів, використання програмних помилок та програмних закладок, використання помилок механізмів ідентифікації користувачів, використання недоліків протоколів передачі даних, отримання інформації про користувачів за допомогою стандартних операційних систем, блокування службових функцій атакованої системи.

На нашу думку, можна виділити чотири типи кіберзлочинів: несанкціонований доступ, зловмисна вірусна модифікація, перехоплення інформації та комбіноване невикористання. Важливо зазначити, що службовці банків (так звані внутрішні користувачі) здійснюють близько 60% злочинів, тоді як зовнішні суб'єкти – лише 40%. У процесі «внутрішніх» перевірок порушень порядку здійснення банківських операцій працівники служб охорони банків виявляють близько 10–15% шахрайства, вчиненого уповноваженими працівниками банків [3, с. 359].

Таким чином, наслідки кіберзлочинності можна розділити на три основні групи:

1) спотворення (несанкціоноване модифікування) даних;

2) проникнення інформації;

3) відмова в обслуговуванні (порушення доступу до мережевих послуг).

Відповідно, завдається шкода цілісності, конфіденційності та доступності інформації. Наслідком значної кількості кіберзлочинів у банківському секторі є зниження довіри населення до надійності фінансової системи, інституту банківської таємниці, надійності захисту персональних даних, а також фінансових операцій із використанням новітніх технологій. Водночас недовіра суспільства до ринків фінансових послуг не дозволяє активно використовувати вільні кошти громадян як інвестиційні ресурси, спрямовані на економічний розвиток. А. Бухтіарова та А. Гуща пропонують поділити наслідки кіберзлочинності на банківську систему на такі групи: фінансові, іміджеві (репутаційні), юридичні, технологічні [3, с. 104].

До негативних факторів, що знижують ефективність боротьби з кіберзлочинністю в Україні, належать: відсутність достатньої державної фінансової підтримки для фундаментальних та прикладних вітчизняних досліджень у галузі запобігання та протидії кіберзлочинності; українське виробництво конкурентоспроможних засобів інформатизації та комунікації та їх захист поволі розвивається; інформатизація державних і комерційних організацій здійснюється переважно на основі зарубіжних технологій та комп'ютерних технологій (стратегічна техніко-технологічна залежність від інших держав).

Доцільно використовувати досвід інших країн щодо запобігання, виявлення, припинення та розслідування кіберзлочинів у банківському секторі.

Аналіз практики розслідування кіберзлочинів у банківському секторі показує, що необхідно запровадити новий підхід до виявлення та розслідування кіберзлочинності, оскільки заходи та методи, що застосовуються для документування традиційних злочинів, неефективні в цій галузі. Таким чином, галузь високих технологій вимагає науково-технічних та інших спеціальних знань не тільки фахівців, а й оперативних працівників, слідчих, прокурорів, слідчих суддів та суддів. У зв'язку з цим особливу увагу слід приділити підвищенню рівня професійної підготовки відповідних оперативних підрозділів, органів досудового розслідування та прокурора. Це пов'язано з тим, що недостатній рівень такої підготовки призводить до помилок у застосуванні кримінально-процесуального та кримінального законодавства.

Цю ситуацію потрібно постійно оновлювати, слід оновлювати існуючі методи розслідування кіберзлочинів та розробляти нові методи розслідування кіберзлочинів у банківському секторі.

Кіберзлочинність за своєю природою є транскордонним явищем, що дозволяє більшості вчених відзначити, що кіберзлочинність характеризується максимальним рівнем латентності. Фактори неефектовної протидії кіберзлочинності такі:

1) складність механізму кіберзлочинності у поєднанні з дуже різноманітними польовими та кримінальними наслідками, а також «комп'ютерна безграмотність» більшості потенційних жертв кіберзлочинності, нехтування їх безпекою;

2) негативна поведінка потерпілих (очевидців) злочину, тобто відмова жертви та осіб, які знають про злочин, до правоохоронних органів та не повідомлення про факт вчинення кіберзлочинів;

3) недоліки в роботі правоохоронних органів при реагуванні на звернення та повідомлення про кіберзлочини [7, с. 163].

Стандартна практика для організацій, які постраждали від кіберзлочинності, – повідомляти про випадки кібератак урядовим чи правоохоронним органам. Однак 28% організацій в Україні відповіли, що навряд чи або навряд чи повідомлять про такі факти урядові чи правоохоронні органи (порівняно з 12% респондентів у всьому світі) [8, с. 167].

Україна приймає відповідні закони та інші нормативні акти, що регулюють відносини у сфері протидії кіберзлочинності. Станом на сьогодні нормативна база кібербезпеки України включає такі документи: Конституція України, Кримінальний кодекс України, закони України «Про основні засади кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України» та інші закони, Доктрина інформаційної безпеки України, Конвенція про кіберзлочинність та інші міжнародні угоди, згода на обов'язковість яких надана Верховною Радою України.

Водночас експерти відзначають проблему недосконалого правового регулювання та реалізації кримінальної відповідальності за кіберзлочинність, неефективну діяльність органів державної влади, до повноважень яких належить боротьба з кіберзлочинністю тощо. До пріоритетних

напрямів кібербезпеки банківської системи України належать, зокрема, захист інформаційних ресурсів банку з урахуванням практики розвинених країн; створення системи навчання в галузі кібербезпеки в банках; моніторинг кіберпростору для своєчасного запобігання кіберзагрозам; розвиток міжнародного співробітництва у галузі кібербезпеки тощо [3, с. 360].

Факторами, що сприяють зростанню кіберзлочинності, є розвиток та вдосконалення ІТ-технологій, значна географія вчинення злочинів, недостатня теоретична та практична підготовка правоохоронців та недосконалість вітчизняного законодавства.

У цьому відношенні слід зазначити, що для України важливо не просто вдосконалити законодавство у сфері боротьби з кіберзлочинністю, а й врахувати людський фактор. Кібербезпека країни більшою мірою залежить від діяльності держави, проте фахівці, що працюють у галузі запобігання, протидії та розслідування кіберзлочинів, відіграють значну роль у створенні ефективної системи кібербезпеки. Потрібен час для врегулювання питання щодо підвищення кваліфікації правоохоронців у галузі ІТ-технологій. Одним із варіантів вирішення цього питання може бути залучення спеціалістів – програмістів, розробників додатків для оплати товарів і послуг, тестувальників програмного забезпечення, системних аналітиків, фахівців із кібербезпеки. Провідна діяльність цих фахівців сприяє постійному професійному зростанню та вдосконаленню навичок відповідно до технологічних змін. Взаємодія правоохоронців з ІТ-спеціалістами частково вирішить питання розслідування злочинів у банківському секторі в кіберпросторі.

У контексті вдосконалення правового регулювання розслідування кіберзлочинів у банківському секторі нині для України важливо перейняти досвід країн з ефективними системами кібербезпеки.

Значна кількість банківських установ в Україні вважає за краще подолати наслідки кіберзлочинності, а не інвестувати в пошук захисту даних та рахунків своїх клієнтів.

Практика розслідування кіберзлочинів в Індії, де до процесу можуть бути залучені професійні хакери, цікава в контексті досліджень. Зараз у багатьох країнах існує так званий кіберкорпус, діяльність якого спрямована на захист кіберпростору країни. Такі корпуси діють у Німеччині, Великобританії, Естонії, США та Китаї. Наприклад, у Німеччині в даний час Кіберкорпус складається з 260 ІТ-спеціалістів.

Міжнародне співробітництво щодо боротьби з кіберзлочинністю повинно здійснюватися на основі участі всіх країн, що визначається характером самої інформації як об'єкта посягання та характером скоєних злочинів. В Україні існує Стратегія кібербезпеки, затверджена Президентом України у 2016 році, згідно з якою антикіберзлочинні заходи повинні включати, зокрема, здійснення заходів щодо вдосконалення процесуальних механізмів збору доказів, що стосуються злочинів, в електронній формі, вдосконалення класифікації, методів, засобів та технологій виявлення та реєстрації кіберзлочинів, проведення експертних досліджень.

Слід зазначити, що існує потреба у подальшому вивченні розслідування кіберзлочинів у банківському секторі через стрімкий розвиток технологій, нових форм та методів вчинення злочинів у кіберпросторі, а також поширення злочинів у банківському секторі. За даними 2020 року, згідно із дослідженням щодо Національного індексу кібербезпеки (NCSI) Україна посідає за рейтингом 25 місце. Очолила рейтинг Греція. У топ-10 входять також Чехія, Естонія, Литва, Іспанія, Бельгія, Фінляндія, Словаччина, Хорватія та Франція. Останню сходинку посів Південний Судан [9].

Таким чином, за результатами глобального дослідження економічних злочинів та шахрайства, проведеного у 2018 році, кіберзлочинність входить до п'ятірки найкращих злочинів в економічній сфері [10].

Висновки. Виходячи з вищесказаного, можна зробити висновок, що кіберзлочинність стає все більш глобальною, де новітні технології сприяють анонімності злочинців, а перспектива швидкого збагачення стимулює все більше людей приєднуватися до цієї злочинної діяльності. Банківська система України – одна із сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та Інтернету. А враховуючи те, що ці технології використовуються для грошових переказів, ця сфера привертає все більше уваги з боку злочинців. Незважаючи на всі заходи, вживані приватними особами, фірмами та державою, кіберзлочинність продовжує діяти, збільшуючи прибуток порушників та зменшуючи вміст кишень звичайних громадян. Ось чому сьогодні особливо важливо переглянути всі існуючі заходи та активно розробляти нові, які принесуть більші переваги та надійніший захист від кіберзлочинців. Ефективна протидія кіберзлочинності повинна поєднувати комплекс правових (законодавчих), технічних, організаційних та інформаційних заходів.

На наш погляд, серед питань ефективної протидії кіберзлочинності і сьогодні актуальними є такі:

1. Розроблення норм права для проведення обшуку електронних доказів з урахуванням можливості їх виявлення в різних юрисдикціях.
2. Розроблення спеціалізованого програмного та апаратного забезпечення для збору, зберігання та аналізу електронних доказів, включаючи великі справи з комп'ютерними доказами.
3. Організація тісної співпраці між правоохоронними органами та постачальниками для отримання електронних доказів.
4. Регулярне підвищення кваліфікації слідчих та інших залучених правоохоронців з метою вивчення актуальних питань тактики проведення слідчих дій з метою отримання електронних доказів у розслідуванні кіберзлочинів.
5. Підвищення рівня кібербезпеки як у державному, так і в приватному секторах, а також розроблення нових технологій захисту та ідентифікації користувачів кіберпростору.
6. Налагодження співпраці між банківськими установами, урядом та правоохоронними органами з погляду як моделей взаємодії, так і підвищення рівня довіри приватного сектору до державних службовців та правоохоронців, що допоможе відобразити реальну статистику кіберзлочинів, скоєних у банківському секторі, та підвищити ефективність його розслідування.
7. Створення українських кіберсил, діяльність яких буде спрямована на попередження та боротьбу зі злочинами, скоєними у кіберпросторі.

Повністю захиститися від кібератак неможливо. Однак дотримання принаймні мінімальних правил безпеки мережі значно збільшить шанси на те, що злочинці не зламають систему. Під час проведення транзакцій між банками або в системі «клієнт-банк» в інтернет-банкінгу важливо використовувати криптологічні інструменти, такі як ключі AES з різними бітрейтами, і чим вище бітрейт, тим більший захист. Впровадження та виконання цих заходів дозволить повною мірою отримати переваги цифрового суспільства.

ЛІТЕРАТУРА

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.03.2021).

2. Всесвітнє дослідження економічних злочинів та шахрайства 2018: результати опитування українських організацій. URL: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html (дата звернення: 25.03.2021).

3. Бухтіарова А.Г., Гуща А.В. Протидія кіберзлочинності у банківській сфері. *Приазовський економічний вісник*. 2019. № 3 (14). С. 355–361.

4. Пацера М. Кіберзлочинність – загроза банківській системі. *Вісник Національного банку України*. 2015. С. 55–59.

5. Карткові шахраї обікрали українців за рік на 360 млн. 2020. URL: https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikraly-ukrayintsiv-za-rik-na-360-mln?utm_source=telegram&utm_medium=social&utm_campaign=co_vsk&utm_content=kartk-shahrai_160220 (дата звернення: 25.03.2021).

6. Сучасне банківництво: теорія і практика : навч. посібник. Ужгород : Видавництво УжНУ «Говерла», 2018. 364 с.

7. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2(19). С. 155–166.

8. Хамига Ю.Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації. Кваліфікаційна наукова праця на правах рукопису. 2020. 292 с.

9. Україна посіла 25 місце у міжнародному рейтингу з кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України. 2020. URL: https://cip.gov.ua/ua/news/ukrayina-posila-25-misce-u-nacionalnomu-indeksi-kiberbezpeki-2020?fbclid=IwAR1LwGfWM7nFs8A3S6weuDIGAyAjmW76uN0uEvZlEXxVLQYXZS0U0eClD28 (дата звернення: 25.03.2021).

10. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій. 2018. URL: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf (дата звернення: 25.03.2021).