Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»
№ 4 (40), 2023

УДК 342

Ірина Хомишин
Національний університет «Львівська політехніка»,
заступниця директора з науково-педагогічної роботи
Навчально-наукового інституту права,
психології та інноваційної освіти,
доктор юридичних наук, професор
iryna.y.khomyshyn@lpnu.ua
ORCID ID :https://orcid.org/0000-0002-6180-347

Оксана Гавц
Національний університет «Львівська політехніка»,
студентка IV-го курсу зі спеціальності «Право»
Навчально-наукового інституту права,
психології та інноваційної освіти
oksana.havts.pv.2020@lpnu.ua

КІБЕРБЕЗПЕКА БАНКІВСЬКОЇ СФЕРИ УКРАЇНИ: ПОНЯТТЯ, ПРОБЛЕМИ ТА ДОСВІД ЗАРУБІЖНИХ ДЕРЖАВ

http://doi.org/10.23939/law2023.40.170

Стаття присвячена аналізу сучасного стану та викликів у сфері кібербезпеки банківського сектору України. В роботі розглядаються ключові поняття та основні аспекти кібербезпеки в контексті банківської сфери, особливо з огляду на зростаючі вимоги до захисту даних та фінансових операцій у цифровому просторі. Детально аналізуються проблеми, з якими стикається банківська сфера України у контексті кібербезпеки, зокрема питання регулювання, управління ризиками, інвестиції у захист інформаційних систем та протидія кіберзлочинності.

Окрему увагу в статті присвячено досвіду зарубіжних держав у сфері кібербезпеки банків. Проаналізовано, як зарубіжні держави реалізовують передові практики та технології для захисту своїх систем і клієнтських даних. Вказано на можливі напрями для поліпшення кібербезпеки в українському банківському секторі.

Завершується стаття висновками та рекомендаціями щодо розвитку стратегії кібербезпеки для банківської сфери України, з врахуванням як внутрішніх викликів, так і досвіду міжнародних партнерів. Підкреслено потребу зміни парадигми «розслідування кіберзлочинів» на «попередження кібер-ризиків».

Ключові слова: банківська сфера; кібербезпека; кібер-ризик; кіберзлочини; шахраї; концепція.

Постановка проблеми: У сучасному світі найважливішим конкурентним фактором у банківському секторі є впровадження інновацій та розвиток інформаційних технологій. Однак цей процес супроводжується також появою нових видів шахрайства. Найбільший інтерес для кіберзлочинців

становить фінансовий сектор. Проблема розвитку кіберзлочинності є вкрай актуальною та злободенною внаслідок масштабів втрат, яких щорічно зазнають кредитні організації у всьому світу. Однак на поточному етапі моделювання кібер-ризиків, також у банківському секторі, розвинене слабо через новизну проблеми, відсутність історичної практики боротьби з кіберзлочинністю на рівні окремих організацій, а також складності в аналізі та оцінці цього виду ризиків.

Аналіз дослідження проблеми. Окремі аспекти вказаного питання досліджували у своїх працях такі фахівці: М. В. Баханова, О. А. Криклій, О. В. Кузьменко, В. О. Тімашов, Н. В. Трусов та ін. Водночас роботи більшості фахівців присвячені переважно економічному або технічному аспекту щодо забезпечення кібербезпеки банківської сфери. Проблематика правових механізмів кібербезпеки у сфері банківської діяльності (навіть з урахуванням міжнародного досвіду) практично не розглядалася.

Мета статті полягає у напрацюванні концепції кібербезпеки банківської сфери України, яка б стала основою у створенні ефективної, вдосконаленої системи захисту та забезпечила б надійну безпеку інформаційних систем і даних у банківській індустрії.

Виклад основного матеріалу. Поняття кібербезпеки є порівняно новим, тому немає загальноприйнятого визначення.

Під кібератакою розуміється навмисне організована сукупність дій за участю програмно-технічних засобів, спрямована на завдання економічного, технічного або інформаційного збитку [1, с. 49]. Отже, спираючись на подані визначення, можна сформулювати поняття кібербезпеки, як комплекс дій стратегічного характеру, спрямований на захист від завдання економічної, технічної чи інформаційної шкоди внаслідок загроз, що здійснюються за допомогою програмно-технічних засобів, а також внаслідок щоденної роботи з інформаційними мережевими технологіями. Кібербезпека забезпечує захист від виникнення збитків через дії зловмисників, які здійснюються за допомогою телекомунікаційних технологій, тобто бореться з проявом кібер-ризиків.

До основних характеристик кібер-ризиків належать:

1. ІТ-природа. Кібер-ризик характеризується як інформаційно-технологічна категорія, посідаючи певне місце у сучасній економіці і продовжуючи все більше проникати у сферу економічної діяльності підприємств, комерційних банків та інших суб'єктів. Еволюція інформаційних технологій є головною передумовою розвитку кібер-ризиків.

2. Об'єктивність прояву. У зв'язку з тим, що в світі практично будь-яка діяльність на підприємствах і в банках супроводжується застосуванням ІТ-технологій, то кібер-ризик є об'єктивним явищем, тобто супроводжує усі операції. Незалежно від того, що низка параметрів кібер-ризику залежить від суб'єктивних управлінських рішень, властивість його об'єктивного прояву залишається незмінною.

3. Імовірність виникнення. Сутність полягає в тому, що в процесі фінансово-господарської діяльності підприємств (банків) кібер-ризик може здійснитися, а може й ні. Ймовірність того, що відбудеться кібератака, визначається дією різних об'єктивних і суб'єктивних факторів, проте імовірнісна належність кібер-ризику є його стійкою характеристикою [2, с. 111–112].

4. Непередбачуваність виникнення. Кібер-ризик складно прогнозований і супроводжується труднощами в оцінці через крайню прихованість кіберзлочинців. Шахраї володіють цією перевагою, яка досягається застосуванням різних механізмів шифрування і анонімності.

5. Очікувана несприятливість наслідків. Ризик у фінансово-господарській діяльності характеризується і співвідноситься з рівнем можливих негативних наслідків. Однією з основних характеристик кібер-ризику є те, що він завжди пов'язаний з якими-небудь несприятливими результатами. Найчастіше кібер-ризики можуть призводити не тільки до втрати прибутку, а й капіталу підприємства (банку), що своєю чергою є причиною банкрутства.

6. Мінливість рівня. Рівень кібер-ризику не завжди однаковий. Знижується в часі і залежить від безлічі об'єктивних і суб'єктивних факторів (наприклад, від якості програмного забезпечення; рівня захисту від кіберзагроз підприємства (банку); кваліфікації персоналу і т.д.) [3, с. 112].

7. Суб'єктивність оцінки. Незважаючи на те, що кібер-ризик є об'єктивним за своєю суттю, його оцінний показник – рівень ризику – має суб'єктивний характер. Ця суб'єктивність (неоднозначність оцінки) характеризується різним рівнем якості інформації, її достовірності та повноти; кваліфікацією співробітників відділу ризик-менеджменту, їх компетентністю та досвідом, а також іншими факторами.

8. Транскордонність. Однією з найважливіших характеристик кібер-ризику є необмеженість у просторі [4, с. 76]. Таким чином, кібершахрай і постраждала від нього сторона можуть перебувати на відстані тисяч кілометрів, що не завадить скоєнню злочину.

Найактуальнішим питання розвитку кіберзлочинності залишається, зокрема, для світового банківського співтовариства. Так, за статистикою, у 2018 році сумарні збитки компаній у всьому світі від кібератак досягли 1,5 трлн. $, а в 2019 році збитки світової економіки перевищили 2 трлн. $

Згідно зі статистикою, наведеною ООН, щорічний економічний збиток від розкрадання онлайн-даних у банківському секторі становить понад 100 млрд. $. [5] До викраданих даних відносяться відомості про кредитні карти, паролі, логіни та інші особисті параметри клієнтів кредитних установ.

За результатами дослідження, проведеного PwC у 2018 році, 31 % організацій в Україні зазнали наслідків кіберзлочинності. Більше третини цих організацій постраждали від зловмисного програмного забезпечення. Кібератаки в Україні призвели не тільки до порушення бізнес-процесів, але й спричинили значні фінансові втрати для організацій. Це підкреслює важливість кібербезпеки для українських підприємств та організацій [6].

Проте, за словами А. Г. Бухтіарової та А. В. Гущі, в банківському секторі кількість кіберзлочинів може бути значно вищою, ніж офіційно повідомляється. Часто кібератаки не є успішними і виявлені вразливості в системах електронного банкінгу швидко усуваються. Розголошення інформації про спроби кібершахрайства може негативно вплинути на рівень довіри клієнтів до банку та призвести до масового вилучення банківських депозитів, створюючи серйозну проблему ліквідності для банків. Тому точна оцінка рівня кіберзлочинності у банківському секторі є невідомою [7, с. 358].

Традиційною темою кіберзлочинності є злочини, пов'язані з банківськими картками, серед яких особливо поширений скіммінг. Скіммінг включає в себе використання спеціальних пристроїв для зчитування інформації з пластикових карток. В Україні у 2013 році було виявлено 293 скіммінг-пристроїв у банкоматах, а у 2019 році – 100 таких пристроїв, з цього приводу було порушено 14 кримінальних справ за 50 фактами [8].

Шахрайство в системах віддаленого банку є однією з форм кіберзлочинності. Цей тип злочинності виникає, коли зловмисники отримують несанкціонований доступ до банківських систем чи інших електронних фінансових платформ, щоб вчинити шахрайські дії. Злочинці можуть використовувати різні методи, такі як фішинг (надмірне впливання на користувачів для отримання їхніх конфіденційних даних), введення шкідливих програм (наприклад, троянців чи шпигунського програмного забезпечення) або експлойти уразливостей в програмному забезпеченні.

Після успішного доступу до систем банку зловмисники можуть виконувати різноманітні банківські операції без дозволу власників рахунків, такі як переказ коштів, зміна персональних даних або інші маніпуляції, спрямовані на виведення грошей [9, с. 103].

Вішинг (від англ. «voice» – голос і «phishing» – шахрайство) – це вид шахрайства, де використовується мобільний телефон або інші засоби голосового зв'язку для обману людей з метою отримання конфіденційної інформації, такої як дані банківських рахунків або персональні дані. При вішингу шахраї часто представляються співробітниками банку, правоохоронних органів, або інших довірених організацій. Вони можуть створити тиск або викликати страх у жертви, змушуючи її

розкрити особисту інформацію або виконати якісь фінансові дії, такі як переказ коштів або надання даних банківської картки.

«Фітинг» теж являється видом онлайн-шахрайства, де зловмисники створюють дублікати реальних веб-сайтів (так звані «фішингові сайти») для введення в оману користувачів і збору їх конфіденційної інформації, такої як дані банківських карток. Коли клієнт вводить свої дані на такому фальшивому сайті, ця інформація потрапляє до зловмисників, які можуть використовувати її для викрадення коштів з рахунку [9, с. 104].

Зважаючи на вище викладене, для фінансових організацій, в контексті нашого дослідження конкретно для банків, дуже важливо забезпечення кібербезпеки та ефективне управління кібер-ризиками, яке допоможе знизити кількість і ймовірність загроз з боку кібершахраїв і звести до мінімуму величину втрат від даних загроз.

Згідно з доповіддю «Управління ризиками та кібербезпекою», підготовленою компанією Price water house Coopers (PwC), основними аспектами кібербезпеки є [6]:

1) визначення рівня допустимого ризику та порогових значень шкоди;

2) визначення прийнятного залишкового ризику та лімітів прийняття;

3) оцінка ризиків необхідної точності та фінансових значень оцінки;

4) встановлення прозорого зв'язку бізнес-процесів і критичних активів;

5) розподіл нових ролей і відповідальності між компетентними фахівцями;

6) визначення допустимих термінів закриття виявлених ризиків;

8) визначення положення кібер-ризиків у системі корпоративного управління ризиками;

9) відповідність рівнів прийняття рішень повноваженням осіб;

10) регулярне надання особам, які приймають рішення, достовірної звітності про кібер-ризики.

Значний внесок у розвиток практичних аспектів забезпечення кібербезпеки в банківській сфері зроблено завдяки міжнародним фінансовим організаціям та органам банківського регулювання та нагляду. Це включає використання раніше розроблених національних та міжнародних стандартів, які служать основою для забезпечення безпеки інформаційних систем у фінансовій сфері. До найважливіших з них можемо віднести:

1. Рамки кібербезпеки Національного інституту стандартів і технологій США (NIST): Ці рамки включають набір стратегій, процедур та технологій, які організації можуть використовувати для управління та зниження ризиків у сфері кібербезпеки. Вони охоплюють різні аспекти, від ідентифікації потенційних загроз до реагування на інциденти кібербезпеки.

2. Серія стандартів ISO 27000: Ця серія міжнародних стандартів встановлює вимоги до систем управління інформаційною безпекою (ISMS). Вона допомагає організаціям захищати свої інформаційні активи таким чином, щоб забезпечити конфіденційність, цілісність та доступність інформації.

3. Керівництво CPMI-IOSCO 2016 (Committee on Payments and Market Infrastructures – International Organisation of Securities Commissions): Це керівництво спрямоване на забезпечення кіберстійкості інфраструктури фінансового ринку, включаючи платіжні системи, розрахункові системи, центральних контрагентів і реєстрів цінних паперів. Воно визначає ключові стандарти та практики, що допомагають цим організаціям ефективно протистояти кіберзагрозам [10].

Група Світового банку, відповідаючи на зростаючі кіберзагрози, розробила збірник нормативних документів, який є важливим ресурсом для фінансового сектора у контексті кібербезпеки. Цей збірник узагальнює наявні нормативні та наглядові практики, включаючи закони, постанови, керівні принципи та інші ключові документи, які стосуються кібербезпеки у фінансовому секторі. Основна мета такого збірника – надати фінансовим інститутам, регуляторам та іншим зацікавленим сторонам зрозумілі та ефективні настанови для захисту від кіберзагроз [11].

У 2018 році Європейський центральний банк (ЄЦБ) опублікував важливий документ під назвою «Очікування щодо нагляду за кіберстійкістю» (CROE), який швидко став важливим ресур-

сом для операторів фінансової інфраструктури в Європі. Цей документ містить рекомендації та очікування відносно забезпечення кіберстійкості в фінансовому секторі. Основні аспекти CROE включають:

1. Створення сильних політик кібербезпеки: Настанови зосереджуються на розробці та впровадженні ефективних політик кібербезпеки, які відповідають потребам конкретної організації та забезпечують адекватний рівень захисту.

2. Управління ризиками та відновлення після інцидентів: Підкреслюється важливість оцінки та управління кіберризиками, а також розробки планів відновлення після інцидентів, щоб мінімізувати вплив потенційних кібератак.

3. Залучення вищого керівництва: Високий рівень участі та залучення вищого керівництва у процеси кібербезпеки вважається ключовим для успішного управління кіберризиками.

4. Неперервне тестування та оцінка систем: Регулярне тестування і оцінка систем безпеки дозволяють своєчасно виявляти слабкі місця та вживати заходів для їх усунення [12].

Світовий банк прийняв CROE як частину своєї глобальної ініціативи щодо фінансової доступності (FIGI), підкреслюючи глобальну важливість цих рекомендацій. Таке прийняття сприяло гармонізації практик кібербезпеки на міжнародному рівні, забезпечуючи більш стійкий та безпечний фінансовий сектор [13].

Як доповнення до CROE, Європейський центральний банк (ЄЦБ) розробив стандарт TIBER-EU (Threat Intelligence-based Ethical Red Teaming). TIBER-EU спрямований на оцінку стійкості фінансового сектора Європейського союзу до кібератак за допомогою симуляції їх наслідків на критичні системи. За допомогою метода «етичний злом», при якому спеціально підготовлена «червона команда» проводить контрольовані кібератаки на фінансові установи, імітуються дії справжніх хакерів. Це дозволяє оцінити, наскільки добре установи готові протистояти реальним кібератакам [14].

Що стосується національного законодавства, то Закон України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року є ключовим документом у сфері кібербезпеки в Україні. В ньому впроваджено низку термінів, пов’язаних із кібербезпекою, а також визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі [15].

Згідно з Законом України «Про Національний банк України», НБУ відіграє ключову роль у розвитку та регулюванні електронних банківських технологій в Україні [16]. Зокрема, саме НБУ розробляє та підтримує роботу платіжних систем, які є важливими для ефективного та безпечного здійснення фінансових операцій в країні. Також НБУ розробляє норми та стандарти, які регулюють захист інформації в банківському секторі, щоб забезпечити конфіденційність та безпеку банківських даних.

Постанова Правління Національного банку України від 12 серпня 2022 року № 178 є одним із останніх здобутків нашої держави в сфері кіберзахисту банківської сфери. Вона була розроблена у відповідності з Законом України «Про основні засади забезпечення кібербезпеки України» та Стратегією кібербезпеки України. Основні аспекти цієї постанови включають:

1. Встановлення чітких рамок та принципів для організації та функціонування системи кіберзахисту в банківському секторі.

2. Визначення механізмів обміну інформацією про кіберзагрози та інциденти між Центром кіберзахисту Національного банку і банками України, що сприяє швидкому реагуванню та координації зусиль.

3. Встановлення конкретних вимог до заходів безпеки, які мають бути реалізовані для захисту критично важливих інформаційних систем в банківському секторі.

4. Встановлення обов’язку для банків проводити незалежні аудити своїх систем інфор-маційної безпеки, щоб гарантувати відповідність стандартам та виявити потенційні слабкі місця [17].

Проте наявність цілого ряду нормативно-правових актів, нажаль не виключає того, що на практиці все одно буваю проблеми. Зокрема, 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).

Вважаємо, що використання досвіду інших країн у сфері запобігання, виявлення, припинення та розслідування кіберзлочинів у банківському секторі є дуже доцільним. Це дозволяє впроваджувати перевірені та ефективні стратегії, що були розроблені та успішно застосовані в інших країнах. Зокрема, цікавим є досвід щодо практика розслідування кіберзлочинів. Так, в Індії, до цього процесу можуть бути залучені професійні хакери, що є цікавим прикладом інноваційного підходу до кібербезпеки. Це відображає глобальну тенденцію залучення фахівців з глибокими технічними знаннями для боротьби з кіберзагрозами.

У багатьох країнах сьогодні існує так званий «кіберкорпус» або аналогічні структури, які спрямовані на захист кіберпростору країни. Кіберкорпус у Німеччині складається з 260 ІТ-спеціалістів, які займаються різними аспектами кібербезпеки, включаючи захист від кібератак та розслідування кіберзлочинів. У Великобританії існують спеціалізовані кібервідділи, які працюють у межах правоохоронних органів та інших державних структур, фокусуючись на протидії кіберзагрозам. Естонія відома своїм високим рівнем кібербезпеки та активною роботою в цьому напрямку, включаючи розвиток національного кіберкорпусу. У США існує ряд урядових агенцій, які відповідають за кібербезпеку, включаючи Національний центр кібербезпеки та комунікацій [18, с. 229].

Важливим також є міжнародне співробітництво у сфері боротьби з кіберзлочинністю, оскільки кіберзлочини часто мають транснаціональний характер і можуть впливати на багато країн одночасно. Характер інформації як об'єкта посягання та міжнародний характер більшості кіберзлочинів вимагають координованих зусиль на глобальному рівні. Ми вважаємо, для ефективної боротьби з кіберзлочинністю країни повинні активно співпрацювати у таких напрямках:

– обмін інформацією про кіберзагрози, тактики злочинців та кращі практики може підвищити здатність країн протистояти кіберзлочинності.

– участь у міжнародних угодах та ініціативах, співпраця з міжнародними організаціями, такими як Інтерпол та Європол.

– розробка спільних стандартів та проведення спільних навчань для правоохоронних органів в сфері кіберзлочинів.

Висновки. Розвиток інформаційних технологій, що відбувається в сучасному світі, несе за собою негативні наслідки у вигляді розвитку кіберзлочинності, яка не стоїть на місці і постійно породжується новими видами атак, інструментів і методів, які дозволяють шахраям проникати в найбільш складні та контрольовані середовища, завдавати великої шкоди і часто залишатися непоміченими. Особливу популярність серед кібершахраїв набув банківський сектор. «Кібер-ризик» представляє для банків одну з найпопулярніших загроз і вимагає до себе особливої уваги. Боротьба з кіберзлочинністю ведеться всіх рівнях: міжнародному, державному, регіональному, галузевому і рівні окремо взятих суб'єктів (зокрема, банків). Проте втрати від кібератак продовжують щорічно збільшуватися і по прогнозах до 2024 року кіберзлочинність коштуватиме світові понад 7 трлн. $ у порівнянні з 3 трлн $ у 2015 році.

Зважаючи на це всім державам, і зокрема Україні необхідно переглядати і вдосконалювати свої концепції захисту банківської сфери. Проаналізована міжнародна та національна нормативно-правова база, доводить, що на законодавчому рівні прийнято багато положень, метою яких є досягнення максимальної безпеки банківського простору. Проте, на практиці вони не завжди спрацьовують.

Проаналізувавши міжнародні стандарти та приклади ряду зарубіжних держав, можемо відзначити, що нині державна концепція кібербезпеки банківської сфери України потребує зміщення акцентів. Зокрема, упор має ставитись на попередження «кібер-ризиків», для цього необхідно інвестувати в пошук захисту даних та рахунків своїх клієнтів, а не на подолання наслідків кіберзлочинності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бараненко Р. В. Кібератаки як одна з форм кібертероризму. *Вчені записки ТНУ імені В. І. Вернадського*. Серія: Технічні науки. Том 32 (71). Ч. 1. № 1. 2021. С. 45–50.

2. Віннікова І. І., Марчук С. В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. *Східна Європа: економіка, бізнес та управління* Випуск 5 (16) 2018. С. 110–114.

3. Волосович С. Детермінанти виникнення та реалізації кібер-ризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101–115.

4. Gable K. A. Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Journal of Transnational Law.* 2010. Vol. 43, No. 1. P. 57–118

5. Доповідь Конгресу ООН щодо попередження злочинності та кримінального правосуддя. URL: https://www.unodc.org/congress/ (дата звернення: 06.11.2023).

6. 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: 06.11.2023).

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

8. Карткові шахраї обікрали українців за рік на 360 млн. 2020. URL: https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikralyukrayintsiv-za-rikna360mln?utm_source=telegram&utm_medium=social&utm_campaign=co_vsk&utm_content=kartk-shahrai_160220 (дата звернення: 07.11.2023).

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

10. Cyber-resilience: Range of practices. Basel Committee on Banking Supervision. 2018. URL: https://www.bis.org/bcbs/publ/d454.pdf (дата звернення: 08.11.2023).

11. Financial Sector's Cybersecurity: A Regulatory Digest. The World Bank Group. 2017. URL: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (дата звернення: 08.11.2023).

12. Cyber resilience oversight expectations for financial market infrastructures. European Central Bank. 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (дата звернення: 08.11.2023).

13. World Bank adopts ECB's cyber resilience oversight expectations. European Central Bank. 2020. URL: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html (дата звернення: 08.11.2023).

14. TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming. European Central Bank. 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (дата звернення: 08.11.2023).

15. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст. 403.

16. Про Національний банк України: Закон України від 20.05.1999 № 679-XIV. *Відомості Верховної Ради України (ВВР)*, 1999, № 29, ст. 238.

17. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України: Постанова Національного банку України; Положення від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 09.11.2023).

18. Тімашов В. О., Корольова О. А., Юрченко Д. Г. Правові засади забезпечення кібербезпеки у банківській сфері. *Юридичний науковий електронний журнал*. № 3/2021. С. 226–230.

REFERENCES

1. Baranenko R. V. ***Kiberataky yak odna z form kiberteroryzmu. Vcheni zapysky TNU imeni V. I. Vernadskoho.*** Seriia: Tekhnichni nauky. Tom 32 (71). Ch. 1. No. 1. 2021. P. 45–50. [In Ukrainian].

2. Vinnikova I. I., Marchuk S. V. ***Kiber-ryzyky yak odyn iz vydiv suchasnykh ryzykiv u diialnosti maloho ta serednoho biznesu ta upravlinnia nymy***. Skhidna Yevropa: ekonomika, biznes ta upravlinnia Vypusk 5 (16). 2018. P. 110–114. [In Ukrainian].

3. Volosovych S. ***Determinanty vynyknennia ta realizatsii kiber-ryzykiv***. Zovnishnia torhivlia: ekonomika, finansy, pravo. 2018. No. 3. P. 101–115. [In Ukrainian].

4. Gable K. A. ***Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent***. *Vanderbilt Journal of Transnational Law.* 2010. Vol. 43, No. 1. P. 57–118. [In English].

5. ***Dopovid Konhresu OON shchodo poperedzhennia zlochynnosti ta kryminalnoho pravosuddia***. URL: https://www.unodc.org/congress/ (data zvernennia: 06.11.2023). [In Ukrainian].

6. ***Vsesvitnie doslidzhennia ekonomichnykh zlochyniv ta shakhraistva 2018***: rezultaty opytuvannia ukrainskykh orhanizatsii. URL: https://www.pwc.com/ua/uk/survey/2018/economic-crime-survey.html (data zvernennia: 06.11.2023). [In Ukrainian].

7. Bukhtiarova A. H., Hushcha A. V. ***Protydiia kiberzlochynnosti u bankivskii sferi. Pryazovskyi ekonomichnyi visnyk***. 2019. No. 3 (14). P. 355–361. [In Ukrainian].

8. ***Kartkovi shakhrai obikraly ukraintsiv za rik na 360 mln. 2020***. URL: https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikralyukrayintsiv-za-rikna360mln?utm_source=telegram&utm_medium=social&utm_campaign=co_vsk&utm_content=kartk-shahrai_160220 (data zvernennia: 07.11.2023). [In Ukrainian].

9. ***Suchasne bankivnytstvo: teoriia i praktyka***: navch. posibnyk. Uzhhorod: Vydavnytstvo UzhNU «Hoverla», 2018. 364 p. [In Ukrainian].

10. ***Cyber-resilience: Range of practices. Basel Committee on Banking Supervision. 2018***. URL: https://www.bis.org/bcbs/publ/d454.pdf (дата звернення: 08.11.2023). [In English].

11. ***Financial Sector's Cybersecurity: A Regulatory Digest***. The World Bank Group. 2017. URL: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf (дата звернення: 08.11.2023). [In English].

12. ***Cyber resilience oversight expectations for financial market infrastructures. European Central Bank. 2018***. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (дата звернення: 08.11.2023). [In English].

13. ***World Bank adopts ECB's cyber resilience oversight expectations. European Central Bank.*** 2020. URL: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews200106.en.html (дата звернення: 08.11.2023). [In English].

14. ***TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming***. European Central Bank. 2018. URL: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (дата звернення: 08.11.2023). [In English].

15. ***Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy***: Zakon Ukrainy vid 05.10.2017 No. 2163-VIII. Vidomosti Verkhovnoi Rady (VVR), 2017, No. 45, st. 403. [In Ukrainian].

16. ***Pro Natsionalnyi bank Ukrainy***: Zakon Ukrainy vid 20.05.1999 No. 679-XIV. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1999, No. 29, st. 238. [In Ukrainian].

17. Pro zatverdzhennia Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy: ***Postanova Natsionalnoho banku Ukrainy; Polozhennia vid 12.08.2022*** No. 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (data zvernennia: 09.11.2023). [In Ukrainian].

18. Timashov V. O., Korolova O. A., Yurchenko D. H. ***Pravovi zasady zabezpechennia kiberbezpeky u bankivskii sferi***. Yurydychnyi naukovyi elektronnyi zhurnal. No. 3/2021. P. 226–230. [In Ukrainian].

Дата надходження: 10.11.2023 р.

Iryna Khomyshyn
Lviv Polytechnic National University,

Professor of the Department of Administrative
and Information law
Educational Institute of Law and Psychology,
Sc. D.
iryna.y.khomyshyn@lpnu.ua
ORCID ID: https://orcid.org/0000-0002-6180-347

Oksana Havts
Lviv Polytechnic National University,
Student of the Educational and Research Institite
of Law, Psychology and Innovative Education
oksana.havts.pv.2020@lpnu.ua

CYBER SECURITY OF THE BANKING SECTOR OF UKRAINE: CONCEPTS, PROBLEMS AND EXPERIENCE OF FOREIGN COUNTRIES

The article is devoted to the analysis of the current state and challenges in the field of cyber security in the banking sector of Ukraine. The work examines the key concepts and main aspects of cyber security in the context of the banking sector, especially because of the growing requirements for the protection of data and financial transactions in the digital space. The problems faced by the banking sphere of Ukraine in the context of cyber security are analyzed in detail, including issues of regulation, risk management, investments in the protection of information systems, and countering cybercrime.

The article pays special attention to the experience of foreign countries in the field of cyber security of banks. Analyzes how foreign countries implement best practices and technologies to protect their systems and customer data. This provides possible directions for improving cyber security in the Ukrainian banking sector.

The article ends with conclusions and recommendations regarding the development of a cyber security strategy for the banking sector of Ukraine, taking into account both internal challenges and the experience of international partners. They emphasize the need to change the paradigm of «cyber crime investigation» to «cyber risk prevention».

Keywords: banking sphere; cyber security; cyber risk; cyber crimes; fraudsters; concept.