МЕНЕДЖМЕНТ ІНФОРМАЦІЙНИХ РИЗИКІВ БАНКІВ ЯК УМОВА ЗМІЦНЕННЯ ЇХ ФІНАНСОВОЇ БЕЗПЕКИ

MANAGEMENT OF BANKS' INFORMATION RISKS AS A CONDITION FOR STRENGTHENING THEIR FINANCIAL SECURITY

УДК 336.71:004.056
DOI: https://doi.org/10.32782/dees.8-37

Єгоричева С.Б.[1]
д.е.н., професор,
професор кафедри фінансів,
банківського бізнесу та оподаткування,
Національний університет
«Полтавська політехніка
імені Юрія Кондратюка»
Онищенко С.В.[2]
д.е.н., професор,
професор кафедри фінансів,
банківського бізнесу та оподаткування,
Національний університет
«Полтавська політехніка
імені Юрія Кондратюка»

Yehorycheva Svitlana
National University
"Yuri Kondratyuk Poltava Polytechnic"
Onyshchenko Svitlana
National University
"Yuri Kondratyuk Poltava Polytechnic"

Метою статті є поглиблення наукових підходів до управління інформаційними ризиками для підвищення рівня фінансової безпеки банківських установ. Актуальність теми зумовлена тим, що поступова диджиталізація суспільства означає не лише позитивні наслідки для економічного розвитку, а і пов'язана зі зростанням ризиків, що особливо відчувається у банківській сфері, де вони здатні завдати відчутної шкоди фінансовим інтересам та репутації банків. Інформаційні ризики є складовою операційних ризиків й можуть бути проаналізовані та оцінені з використанням якісних та кількісних методів. У статті розкрито специфіку їх ідентифікації та кількісного оцінювання, надано характеристику загроз інформаційній безпеці банку та вразливостей окремих інформаційних активів. Особливу увагу приділено такому способу мінімізації ризиків, як їх зниження за рахунок удосконалення методів внутрішнього контролю. Розглянуті методи дають змогу оцінити поточний стан інформаційної безпеки банківських установ, знизити потенційні втрати, запропонувати механізм захисту від виявлених загроз, що сприятиме зміцненню фінансової безпеки банків.
Ключові слова: *інформаційні ризики, інформаційна безпека, фінансова безпека, банки, загрози, менеджмент ризиків.*

The purpose of the article is to deepen scientific approaches to information risk management to increase the level of financial security of banking institutions. The relevance of the topic is due to the fact that the gradual digitization of society means not only positive consequences for economic development, but also is associated with the increase of risks, which is mostly found in the banking sector, where they can cause significant damage to the banks' financial security. The latter is understood as the protection of the bank's financial interests; sufficiency of financial resources to achieve defined goals; ensuring financial stability, efficient operation and stable development; the ability to resist negative influences (threats). Information risks are a component of operational risks and can be analyzed and assessed using qualitative and quantitative methods. The article identifies problems related to the quantitative assessment of information risks due to the dynamism of the bank's information environment and the complexity of collecting data. Identification of information assets is recommended to be carried out with reference to the bank's business processes. The article provides a description of threats to the bank's information security, based on the approach of Basel Committee. Among the vulnerabilities of individual information assets, two groups are distinguished, which differ in the mechanism of collecting information about them: those inherent in software and hardware, and those characteristic of business processes and the sphere of control. Among the methods of minimization information risks – acceptance, avoidance, limitation and transfer, special attention is paid to such a method as reducing them due to the improvement of internal control methods. The role of corporate governance in this process is emphasized. The considered methods make it possible to assess the current state of information security of banking institutions, reduce potential losses, and propose a mechanism of protection against identified threats, which will contribute to strengthening the financial security of banks.
Key words: *information risks, information security, financial security, banks, threats, risk management.*

Постановка проблеми. Забезпечення фінансової безпеки в умовах воєнного стану в Україні є фундаментальним завданням всіх суб'єктів національної економіки, оскільки від їхньої здатності зберігати стійкість до зовнішніх і внутрішніх загроз, адаптуватися до безпрецедентних кризових умов залежить спроможність ефективно функціонувати. Водночас, стрімкий розвиток IT-сфери, інтенсифікація використання сучасних інформаційних технологій в усіх сферах економіки, у тому числі, у фінансовій, обумовлюють зростання ролі інформаційної складової у забезпеченні фінансової безпеки. В умовах цифровізації інформаційні активи правомірно вважати стратегічним ресурсом, від цілісності, доступності та конфіденційності якого безпосередньо залежать фінансова стійкість, стабільність й безпека функціонування банківських установ. У той же час, збільшення каналів можливого витоку інформації, зростання частоти та масштабів кібератак, труднощі відновлення складного комп'ютерного обладнання при виході його з ладу, інші загрози інформаційній безпеці призводять до суттєвих фінансових та репутаційних втрат. Необхідність визначення, попередження й нейтралізації цих загроз актуалізує проблему вдосконалення управління інформаційними ризиками банків у контексті зміцнення їхньої фінансової безпеки.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення фінансової безпеки суб'єктів різних рівнів національної економіки широко розглядаються у працях вітчизняних науковців. Зокрема, дослідження О. Барановського [1; 2], Г. Карчевої Г. [3], В. Коваленко [4; 5] присвячені визначенню сутності, складових фінансової безпеки банківської системи та окремих банків,

[1] ORCID: https://orcid.org/0000-0002-7829-7073
[2] ORCID: https://orcid.org/0000-0002-6173-4361

проблемам формування системи її забезпечення та особливостям й шляхам підтримання фінансової безпеки в умовах сучасної України, враховуючи й зростаючі інформаційні ризики. В. Онищенко та ін. [6] аналізують напрями впливу розвитку інформаційних технологій та впровадження інновацій на підтримання фінансової безпеки держави. В. Боженко та ін. [7] розкривають європейський досвід забезпечення кіберстійкості фінансового сектору.

Інформаційні ризики банків стали предметом наукових досліджень вітчизняних учених уже достатньо давно, хоча спочатку вони асоціювалися лише з витоком необхідної для банківської установи інформації, використання нею необ'єктивної інформації або відсутності потрібної, а також поширенням негативних відомостей про банк [8, с. 29]. Дослідження цієї проблематики суттєво активізувалося на початку 2010-х років, разом із затвердженням Національним банком України у 2010 році стандартів з управління інформаційною безпекою в банківській системі України. Втім, особливістю цих публікацій [9; 10; 11; 12] було зосередження уваги саме на технічних аспектах забезпечення інформаційної безпеки банківських установ, пов'язаних з використанням інформаційно-комп'ютерних технологій.

Пізніше менеджмент інформаційних ризиків став розглядатися невід'ємною частиною управління операційними ризиками комерційних банків, а відтак – складовою забезпечення їхньої фінансової безпеки та стабільної діяльності. Тут варто відмітити публікації Л. Кібальник та І. Напори [13; 14], а також В. Ахрамовича й В. Чегренця [15]. Інформаційні ризики банківської діяльності розглядаються й Д. Гладких в аспекті розвитку інфраструктури безготівкових розрахунків, ринку криптовалют та електронних кредитних платформ [16].

Постановка завдання. Метою статті є розвиток підходів до реалізації менеджменту інформаційних ризиків банків як умови підвищення рівня їхньої фінансової безпеки в умовах диджиталізації економіки. Вирішення цього питання буде сприяти обґрунтованій ідентифікації загроз та оперативному реагуванню на них, а отже, підвищенню рівня інформаційної безпеки банківських установ та забезпеченню їхньої фінансової стійкості.

Виклад основного матеріалу дослідження. У вітчизняній науці фінансова безпека розуміється як складна багатофакторна категорія, що виступає результатом синергетичної взаємодії багатьох процесів, які становлять зміст діяльності економічних суб'єктів. Аналіз наукових праць з цієї проблематики [1–5] дозволяє зробити висновок, що до сутнісних ознак фінансової безпеки банків автори відносять захищеність його фінансових інтересів; достатність фінансових ресурсів для досягнення визначених цілей; забезпечення фінансової стійкості, ефективної діяльності та стабільного розвитку; здатність протистояти негативним впливам (загрозам). Під загрозами розуміються дестабілізуючі чинники, явища і процеси, що можуть негативно впливати на діяльність банку, уражаючи його фінансові інтереси, насамперед, щодо зменшення обсягу капіталу через завдані збитки.

В умовах диджиталізації економіки застосування різноманітних інформаційних технологій є одним з важливих факторів, що визначають конкурентоспроможність банку. Втім, поряд з очевидними перевагами, такими, як підвищення швидкості та якості обслуговування клієнтів, доступності банківських послуг, а також зниження витрат, використання інформаційних технологій породжує нові суттєві загрози, які провокують виникнення інформаційних ризиків (ІР).

Варто зазначити, що у документах Базельського комітету з банківського нагляду не міститься окремих положень щодо інформаційних ризиків, вони включаються до складу операційних, що визначаються як ризик втрат внаслідок неадекватності або збоїв внутрішніх процесів, персоналу та систем або зовнішніх подій [17, с. 965]. Для покращення розуміння цього трактування, Базельський комітет склав список із семи категорій подій, що призводять до збитків, й які банки можуть використовувати під час ідентифікації операційного ризику. Зокрема, шоста категорія – «Порушення роботи та збої у системах» [17, с. 979], до якої відносяться обладнання, програмне забезпечення та телекомунікації, безпосередньо уособлює ІР.

Інформаційні ризики можуть розумітися і більш розширено, як ризики виникнення збитків внаслідок неправильної організації або навмисного порушення інформаційних потоків та систем банку. Таке трактування включає складові ІР, зазначені, зокрема, у роботі [8], тому охоплює досить різнорідні за своєю природою ризики, що вимагають різних підходів до оцінки та управління, які неможливо узагальнити в єдиній методиці.

Тому предметом нашого дослідження є ризики виникнення втрат банку у результаті впливу людей та зовнішніх подій на інформаційні системи, а також внаслідок їхніх збоїв та неадекватної роботи. Таке розуміння ІР відповідає визначенню ризику інформаційної безпеки, що надається Національним банком України: імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку [18]. Зазначається, що ризик інформаційної безпеки включає і кіберризик як ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз [19].

Суттєвість впливу ІР на фінансову безпеку фінансових інститутів підтверджується інформацією щодо середньої вартості витоку даних у фінансовій сфері, що є однією з найвищих серед всіх галузей і займає друге місце після охорони здоров'я (табл. 1).

Виходячи з самого тлумачення інформаційних ризиків, зрозуміло, що їх реалізація має суттєвий вплив на стан фінансової безпеки банків не лише внаслідок прямого зменшення доходів та прибутку, а і через ускладнення реалізації певних бізнес-процесів, що призводить до зменшення обсягу проведення операцій, зокрема, залучених ресурсів, накладання штрафних санкцій, відтоку клієнтів, зниження репутації фінансових установ, послаблення їх конкурентних позицій на ринку. Тому, на вимогу НБУ, менеджмент інформаційних ризиків має стати як складовою системи управління інформаційною безпекою, так і проводитися у рамках системи управління ризиками банку [21]. При цьому банк має право самостійно визначати підходи щодо оцінювання та поводження з ризиками інформаційної безпеки.

Втім, кількісна оцінка ІР ускладнена і часто виявляється неточною і ненадійною з декількох причин, частина з яких відноситься до всіх операційних ризиків, а частина специфічна саме для цього виду ризиків. Насамперед, дані для таких кількісних оцінок, як правило, складно зібрати: це вимагає вичерпного розуміння всіх загроз і характеру їх впливу на велику кількість активів банку, починаючи від інформаційних систем (ІС) і завершуючи репутацією банку. При цьому вимагається точність реєстрації подій, її безперервність і достатньо тривалий період збирання даних. По-друге, інформаційне середовище сучасного банку включає велику кількість об'єктів інформаційних ризиків, які, до того ж, періодично змінюються, вдосконалюються, тому модель інформаційного середовища банку повинна бути максимально гнучкою з можливістю переналаштування. Крім того, докладна оцінка ризиків не може бути загальною для всього банку, вона потребує врахування як загальних для банку проблем, так і конкретних питань для кожного бізнес-процесу. Нарешті, витрати часу та людських ресурсів на аналіз вразливості до ІР і, власне, ризик-аналіз можуть бути значними, що не дозволить проводити його з необхідною періодичністю. Проте зазначені проблеми не заперечують практичної можливості управління інформаційними ризиками, а стимулюють до пошуку нових удосконалених підходів.

Відповідно до загальноприйнятого механізму управління банківськими ризиками, цей процес починається з їхньої ідентифікації, для чого, насамперед, варто провести інвентаризацію інформаційних активів (ІА) та скласти карту інформаційної інфраструктури банку. Під ІА будемо розуміти, з одного боку, різноманітні види банківської інформації (платіжної, фінансово-аналітичної, клієнтської та ін.), програмне забезпечення (software) і навіть репутацію банку, а з іншого – технологічні, матеріальні активи (hardware). Всі ці активи тією чи іншою мірою мають певні вразливості і підпадають під вплив внутрішніх і зовнішніх загроз, а отже є об'єктами інформаційних ризиків.

Оскільки Національним банком передумовою впровадження системи управління інформаційною безпекою визначається упровадження у діяльності банку процесного підходу [21], то і всі інформаційні активи повинні описуватися з прив'язкою до бізнес-процесів, щоб мати можливість отримання консолідованої оцінки ризиків кожного з них. Інша вимога НБУ – щодо запровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки – має реалізовуватися через визначення значимості ІА для реалізації бізнес-процесу, досягнення цілей діяльності банку та його фінансової безпеки, а також ступеня чутливості ІА до загроз, який вимагає певного рівня захисту.

Варто зазначити, що Національний інститут стандартів й технологій США, в якому була розроблена одна з найпопулярніших та широковживаних методик управління ризиками в інформаційних технологіях NIST 800-30, рекомендує виділяти програмні інтерфейси, тобто додатки, що забезпечують взаємодію зовнішніх користувачів і персоналу банку з апаратними засобами та інформаційно-комп'ютерними системами, в окрему групу об'єктів ризику [22]. Це обумовлено їхньою високою значимістю й потенційною схильністю до впливу загроз, оскільки саме через них

Таблиця 1

Середня вартість витоку даних у всьому світі за галузями, млн доларів США

Галузь	Травень 2020 – березень 2021	Березень 2021 – березень 2022	Березень 2022 – березень 2023
Охорона здоров'я	9,23	10,1	10,93
Фінансовий сектор	5,72	5,97	5,9
Освіта	3,79	3,86	3,65
Транспорт	3,75	3,59	4,18
Публічний сектор	1,93	2,07	2,6

Джерело: складено авторами за даними [20]

здійснюється взаємодія людини та інформаційних систем. Особливого значення проблема безпеки програмних інтерфейсів набуває у зв'язку з планами впровадження в Україні до 2025 року концепції відкритого банкінгу (open banking), відповідно до якої банки для покращення обслуговування повинні надати третім сторонам, які беруть участь у наданні платіжних послуг, доступ до визначеного кола даних клієнтів.

Визначення значимості та чутливості ІА має здійснюватися за певною формалізованою шкалою, за основу для якої може братися британська методика GRAMM [23]. Вона оперує десятибальною шкалою і при низькій оцінці (3 бали і нижче) за декількома критеріями рекомендує базовий рівень захисту інформаційних активів, що не передбачає докладної оцінки ризиків.

Наступний етапом в управління інформаційними ризиками є виявлення загроз, тобто факторів ризику. Їхня класифікація має бути єдиною, повною й несуперечливою, й завдання її створення покладається на ризик-менеджерів. Кожен банк може застосовувати свою класифікацію, проте доцільніше покладатися на класифікацію Базельського комітету, що є результатом багаторічного аналізу джерел та типів втрат від операційних ризиків банківських установ в усьому світі [17, с. 977–980]. Відповідно, до загроз, що провокують виникнення інформаційних ризиків, можна, зокрема, віднести ті, що зазначені у табл. 2.

Джерела загроз, що можуть призвести до порушення цілісності, доступності та конфіденційності інформації, повинні бути виявлені та описані з рівнем деталізації, що визначається реальними потребами у захисті, тобто у залежності від співвідношення вартості захисту і обсягу ризику. Тому процес ідентифікації інформаційних ризиків є циклічним, з уточненням інформації, залученням додаткових даних, порівняннями і подальшою деталізацією. Найрізноманітнішими, на нашу думку, є загрози, що походять від людини, що визначає необхідність максимально докладного їх опису.

Проте у ланцюжку «інформаційний актив-загроза-ризик» трансформація загрози у ризик відбувається не автоматично, а при наявності вразливостей, під якими розуміється відсутність або слабкість запобіжних заходів, що дозволяють знизити ризик або взагалі уникнути його. Зокрема, відсутність антивірусного захисту збільшує як частоту ризикових подій, так і обсяги втрат, якщо зараження буде виявлено із суттєвим запізненням, що призведе до необхідності відновлення інформації, переустановлення операційної системи або її окремих модулів тощо.

Для цілей збирання інформації щодо вразливостей ІА й подальшого аналізу, їх можна поділити на дві великі групи:

– вразливості, специфічні для програмних й апаратних засобів, прикладом яких можуть бути слабкості конкретних версій програмного забезпечення або моделей обладнання, допущені розробниками або виробниками;

– специфічні для бізнес-процесів та сфери контролю банку вразливості як наслідок слабкостей практик, що використовуються банківською

Таблиця 2

Приклади загроз, що провокують появу інформаційних ризиків банку

Категорії подій (рівень 1)	Приклади діяльності, що створює загрози
Внутрішнє шахрайство	Несанкціоноване використання інформаційних систем Умисне спотворення (приховування/розкриття) інформації
Зовнішнє шахрайство	Незаконне проникнення в інформаційні системи, у т.ч. через мережу Інтернет (хакерські атаки) Завдання шкоди інформаційним системам Крадіжка інформації, що спричинила грошові втрати
Клієнти, продукти й бізнес-практики	Пов'язане з недосконалістю систем неправомірне розкриття конфіденційної інформації й порушення банківської таємниці
Пошкодження матеріальних активів	Шкода, завдана інформаційним системам внаслідок впливу природних явищ Шкода, завдана інформаційним системам актами тероризму, вандалізму
Порушення роботи та збої у системах	Вихід з ладу банківської інформаційної системи, окремих модулів та елементів її функціоналу Відмови і збої у роботі автоматизованих систем Збої у роботі каналів зв'язку Поломка обладнання (комп'ютери, банкомати, термінали тощо)
Виконання, доставка та управління процесом	Відсутність (недосконалість) системи захисту або порядку контролю доступу до інформації Неправильна організація інформаційних потоків всередині банку Невиконання постачальниками, провайдерами зобов'язань перед банком Помилки при введенні та обробці даних за операціями й угодами Помилки моделей і систем

Джерело: складено авторами на основі [17]

установою для організації і управління інформаційною інфраструктурою та для контролю інформаційної безпеки.

І якщо інформація щодо першої групи вразливостей ІА, як правило, знаходиться у відкритому доступі і повідомляється самими розробниками, то щодо вразливостей другої групи зовнішні джерела інформації практично відсутні, тому варто покладатися на внутрішні експертні опитування у рамках самооцінки рівня інформаційної безпеки банку. При цьому доцільно враховувати положення стандарту COBIT, створеного Асоціацією з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням інформаційними технологіями (США), який містить кращі практики та визначає модель зрілості процесів інформаційної безпеки [24].

Для кількісного оцінювання інформаційних ризиків, що втілюється у визначенні очікуваних втрат за певний період часу (annualized loss expectancy, ALE), необхідно враховувати такі фактори, як вартість інформаційного активу (asset value, AV), ступінь його вразливості (exposure factor, EF) та ймовірність виникнення загроз (annualized rate of occurrence, ARO):

$$ALE = AV \times EF \times ARO.$$

Оцінка ризиків є достатньо складним завданням, оскільки ІА мають, як правило, декілька ціннісних характеристик, на відміну, зокрема, від фінансових активів; втрати можуть набувати різного вигляду; реалізація однієї ризикової події може мати наслідком втрати різних видів; безліч факторів впливає на величину втрат. При оцінюванні величини таких втрат варто мати на увазі не лише безпосередні витрати на заміну обладнання та відновлення інформації, а і величину шкоди, нанесеної бізнес-процесам банку. Ще більш віддаленими, але сильнішими за впливом наслідками є втрата ділової репутації, послаблення конкурентної позиції.

Тому банкам варто використовувати різноманітні методики оцінювання ризиків, які вже напрацьовані у міжнародній практиці забезпечення інформаційної безпеки [15, с. 55]. Вітчизняні фахівці пропонують для цих цілей застосовувати адаптовану для використання у банківський діяльності СУІБ «Матриця» [12]. Втім, враховуючи надзвичайну динамічність змін інформаційного середовища банку у сучасних умовах та високу комплексність його внутрішніх взаємозв'язків, найбільш прийнятним для оцінки інформаційних ризиків можна вважати метод, який дозволяв би використовувати різнорідні за своєю природою дані (експертні оцінки й інформацію про понесені банком збитки) та був би придатним для моделювання причинно-наслідкових взаємозв'язків. На думку науковців [10], таким методом є побудова так званих байєсових мереж на основі теорема Байєса, цінність якої стосовно оцінки ІР полягає в її спроможності комбінувати дані про ймовірність подій, отриманих експертним і статистичним шляхом.

Методи зниження ризиків для кожного об'єкту інформаційних активів банку є стандартними для ризик-менеджменту:

– прийняття ризику. Банк визнає потенційні втрати прийнятними для себе і не впроваджує спеціальні заходи з мінімізації ризику;

– уникнення ризику. Банк ухвалює рішення про усунення відповідної загрози, наприклад, відмовляється від використання встановленого програмного забезпечення, що суттєво порушує вимоги інформаційної безпеки;

– обмеження ризику. Банк запроваджує спеціальні заходи контролю, які знижують ймовірність реалізації загрози ІА або зменшують наслідки цієї реалізації;

– передача ризику. Банк створює умови для компенсації потенційних втрат шляхом передавання ризику третій особі, зокрема, використовуючи страхування або віддаючи окремі функції на аутсорсинг.

Всі ці напрями поводження з інформаційними ризиками не є взаємовиключними і, як правило, застосовуються у комплексі, оскільки серед ризиків є підконтрольні та непідконтрольні банку. Основна мета цієї діяльності – зниження ІР до прийнятного для банківської установи рівня, але оскільки ризик при цьому не усувається повністю, то залишкова його частина має бути прийнята банком у межах визначеного ним ризик-апетиту.

На наш погляд, засоби контролю для обмеження інформаційних ризиків можна поділити на три категорії у залежності від методів впливу на джерело ризику:

– організаційні (управлінські) засоби передбачають створення надійної та гнучкої системи управління ІР (розподіл відповідальності за забезпечення безпеки інформаційних активів, удосконалення методик оцінювання ризиків, забезпечення ґрунтовної підготовки користувачів інформаційних систем, створення механізму реагування в екстрених ситуаціях тощо);

– технічні засоби полягають у використанні автоматизованих механізмів контролю безпеки ІА (зокрема, використання криптографічного захисту інформації, захищених каналів зв'язку, програмних методів автентифікації та авторизації, антивірусного захисту тощо);

– технологічні (операційні) засоби покликані забезпечити та контролювати безперервність функціонування ІА банку (наприклад, контроль фізичного доступу до обладнання, архівування та резервне копіювання інформації, забезпечення безперебійного енергозабезпечення, протипожежний захист тощо).

Слід наголосити, що важливим елементом дотримання політики інформаційної безпеки у банках є корпоративне управління та корпоративна етика. Попередження конфлікту інтересів, розподіл повноважень і ролей, недопущення надання надзвичайних повноважень, контроль за обігом конфіденційної інформації – все це організаційні заходи, значимі для будь-яких видів операційних ризиків, набувають виключного значення для інформаційних ризиків внаслідок їх взаємозв'язку практично з усіма бізнес-процесами банку.

Висновки. Охарактеризовані у дослідженні особливості інформаційних ризиків вимагають, щоб механізми захисту інформаційних активів банку функціонували безперервно, а також регулярно перевірялися на адекватність загрозам, що сприятиме підтриманню фінансової безпеки банківських установ. Актуалізація інформації про фактори ризиків, їх оцінювання й оновлення комплексу заходів з їхньої мінімізації мають проводитися з певною періодичністю, зафіксованою во внутрішніх документах банку, зокрема, в його політиці інформаційної безпеки. Ключовими факторами успіху у процесі реалізації програми зниження інформаційних ризиків є підтримка вищого керівництва банків, наявність документально оформлених процедур всіх етапів управління цими ризиками, чіткий розподіл відповідальності за впровадження засобів контролю, періодичне тестування контрольних інструментів.

Перспективи подальших досліджень цієї проблематики полягають у вдосконаленні методів оцінювання передбачуваних та непередбачуваних втрат банків від інформаційних ризиків, а також шляхів мінімізації наслідків їхньої реалізації, особливо у випадках настання надзвичайних обставин, які знаходяться поза впливом банківських установ.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Барановський О., Лагно А. Природа фінансової безпеки банківської системи. *Світ фінансів.* 2022. № 3(72). С. 141–155.

2. Федорущенко Б., Барановський О. Формування системи забезпечення фінансової безпеки банківського сектору. *Фінансово-кредитна діяльність: проблеми теорії і практики*. 2021. № 5(40). С. 16–27.

3. Карчева Г., Карчева І. Теоретичні та практичні аспекти управління фінансово-економічною безпекою банків. *Економічний аналіз*. 2022. Т. 32. № 1. С. 168–198.

4. Коваленко В. Фінансова безпека банків: реалії та перспективи забезпечення. *Економічний форум*. 2022. № 1(2), С. 141–151.

5. Коваленко В. Фінансова безпека банків в умовах воєнного стану. *Фінансовий простір*. 2022. № 4(48). С. 81–93. URL: http://fpnpu.cibs.ubs.edu.ua/article/view/272736

Onyshchenko V., Yehorycheva S., Maslii O., Yurkiv N. Impact of Innovation and Digital Technologies on the Financial Security of the State. In: Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. *Lecture Notes in Civil Engineering*. 2020. Vol. 181. P. 749–759.

Боженко В.В., Пахненко О.В., Койбічук В В. Досвід ЄС щодо розробки та впровадження національної стратегії кіберстійкості фінансового сектора. *Цифрова економіка та економічна безпека*. 2023. № 8. С. 125–129.

6. Диба М., Зубок М., Яременко С. Інформаційні ризики у банківській діяльності. *Вісник Національного банку України*. 2007. № 9. С. 28–35.

7. Єрмошин В.В., Невойт Я.В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем. *Сучасний захист інформації.* 2014. № 3. С. 26–29.

8. Кузнєцова Н.В. Деякі аспекти мінімізації інформаційних ризиків у банківської діяльності. *Системні дослідження та інформаційні технології.* 2014. № 1. С. 7–19.

Кравченко А.М., Орєхов А.А., Гаркунов А.Г. Особливості захисту інформаційних систем у банківських установах. *Сучасний захист інформації*. 2013. № 2. С. 53–55.

9. Домарєв Д.В., Домарєв В.В. Методика управління інформаційною безпекою в банківських установах за допомогою СУІБ «Матриця». *Безпека інформації*. 2013. Том 19. № 1. С. 60–70.

10. Кібальник Л.О., Напора І.Ю. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки. *Ефективна економіка*. 2016. № 12. URL: http://www.economy.nayka.com.ua/ ?op=1&z=5303

11. Кібальник Л.О., Напора І.Ю. Впровадження політики інформаційної безпеки банківських установ. *Причорноморські економічні студії*. 2016. Вип. 12-2. С. 119–122.

12. Ахрамович В.М., Чегренець В.М. Управління ризиками інформаційної безпеки комерційного банку. *Сучасний захист інформації*. 2019. №2(38). С. 54–59.

13. Гладких Д.М. Банківська безпека держави в умовах розвитку інформаційної економіки (трансформації банківських операцій): монографія. Київ : НУОУ, 2019. 393 с.

14. Basel Committee on Banking Supervision. The Basel Framework. 2023. URL: https://www.bis.org/baselframework/BaselFramework.pdf

15. Положення про організацію системи управління ризиками в банках України та банківських групах : постанова Правління Національного банку України від 11.06.2018 № 64. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text

16. Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг : постанова Правління Національного банку України від 16.01.2021 № 4. URL: https://zakon.rada.gov.ua/laws/show/v0004500-21#Text

17. Average cost of a data breach worldwide from May 2020 to March 2023, by industry. Statista. URL: https://www.statista.com/statistics/387861/cost-data-breach-by-industry

18. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : постанова Правління Національного банку України від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text

19. Stoneburner G., Goguen A., Feringa A. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30. 2002.

20. National Cyber Security Centre. Risk management. A basic risk assessment and management method. 2023. URL: https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method

21. Information Systems Audit and Control Association. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA, 2012. 94 p.

REFERENCES:

1. Baranovskyi O., & Lahno A. (2022) Pryroda finansovoi bezpeky bankivskoi systemy [The nature of financial security of the banking system]. *Svit finansiv – The world of finance,* no. 3(72), pp. 141–155. (in Ukrainian)

2. Fedorushchenko B., & Baranovskyi O. (2021) Formuvannia systemy zabezpechennia finansovoi bezpeky bankivskoho sektoru [Formation of the system of ensuring financial security of the banking sector]. *Finansovo-kredytna diialnist: problemy teorii i praktyky – Financial and credit activity: problems of theory and practice,* no. 5(40), pp. 16–27. (in Ukrainian)

3. Karcheva H., & Karcheva I. (2022) Teoretychni ta praktychni aspekty upravlinnia finansovo-ekonomichnoiu bezpekoiu bankiv [Theoretical and practical aspects of managing the financial and economic security of banks]. *Ekonomichnyi analiz – Economic analysis,* vol. 32, no. 1, pp. 168–198. (in Ukrainian)

4. Kovalenko V. (2022) Finansova bezpeka bankiv: realii ta perspektyvy zabezpechennia [Financial security of banks: realities and prospects of provision]. *Ekonomichnyi forum – Economic Forum,* no. (2), pp. 141–151. (in Ukrainian)

5. Kovalenko V. (2022) Finansova bezpeka bankiv v umovakh voiennoho stanu [Financial security of banks under martial law]. *Finansovyi prostir – Financial space,* no. 4(48), pp. 81–93. URL: http://fpnpu.cibs.ubs.edu.ua/article/view/272736. (in Ukrainian)

6. Onyshchenko V., Yehorycheva S., Maslii O., & Yurkiv N. (2020) Impact of Innovation and Digital Technologies on the Financial Security of the State. In: Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. *Lecture Notes in Civil Engineering,* vol 181, pp. 749–759.

7. Bozhenko V. V., Pakhnenko O. V., & Koibichuk V. V. (2023) Dosvid YeS shchodo rozrobky ta vprovadzhennia natsionalnoi stratehii kiberstiikosti finansovoho sektora [The experience of the EU regarding the development and implementation of the national strategy of cyber resilience of the financial sector]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital economy and economic security,* no. 8, pp. 125–129. (in Ukrainian)

8. Dyba M., Zubok M., & Yaremenko S. (2007) Informatsiini ryzyky u bankivskii diialnosti [Information risks in banking]. *Visnyk Natsionalnoho banku Ukrainy – Bulletin of the National Bank of Ukraine,* no. 9, pp. 28–35. (in Ukrainian)

9. Yermoshyn V.V., & Nevoit Ya.V. (2014) Analiz i otsinka ryzykiv informatsiinoi bezpeky dlia bankivskykh ta komertsiinykh system [Analysis and assessment of information security risks for banking and commercial systems]. *Suchasnyi zakhyst informatsii – Modern information protection,* no. 3, pp. 26–29. (in Ukrainian)

10. Kuznietsova N.V. (2014) Deiaki aspekty minimizatsii informatsiinykh ryzykiv u bankivskoi diialnosti [Some aspects of minimizing information risks in banking]. *Systemni doslidzhennia ta informatsiini tekhnolohii – System research and information technologies,* no. 1, pp. 7–19. (in Ukrainian)

Kravchenko A.M., Oriekhov A.A., & Harkunov A.H. (2013) Osoblyvosti zakhystu informatsiinykh system u bankivskykh ustanovakh [Peculiarities of protection of information systems in banking institutions]. *Suchasnyi zakhyst informatsii – Modern information protection,* no. 2, pp. 53–55. (in Ukrainian)

11. Domariev D.V., & Domariev V.V. (2013) Metodyka upravlinnia informatsiinoiu bezpekoiu v bankivskykh ustanovakh za dopomohoiu SUIB «Matrytsia» [Methodology of information security management in banking institutions with the help of SUIB “Matrytsia”]. *Bezpeka informatsii – Information security,* vol. 19, no. 1, pp. 60–70. (in Ukrainian)

12. Kibalnyk L.O., & Napora I.Yu. (2016) Kontseptualnyi pidkhid do formuvannia informatsiinoi bezpeky bankivskykh ustanov v systemi ekonomichnoi bezpeky [A conceptual approach to the formation of information security of banking institutions in the system of economic security]. *Efektyvna ekonomika – Efficient economy,* no. 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5303. (in Ukrainian)

13. Kibalnyk L.O., & Napora I.Yu. (2016) Vprovadzhennia polityky informatsiinoi bezpeky bankivskykh ustanov [Implementation of the information security policy of banking institutions]. *Prychornomorski ekonomichni studii – Black Sea Economic Studies,* vol. 12-2, pp. 119–122. (in Ukrainian)

14. Akhramovych V. M., & Chehrenets V. M. (2019) Upravlinnia ryzykamy informatsiinoi bezpeky komertsiinoho banku [Information security risk management of a commercial bank]. *Suchasnyi zakhyst informatsii – Modern information protection*, no. 2(38), pp. 54-59. (in Ukrainian)

15. Hladkykh D. M. (2019) Bankivska bezpeka derzhavy v umovakh rozvytku informatsiinoi ekonomiky (transformatsii bankivskykh operatsii) [Banking security of the state in the conditions of the development of the information economy (transformation of banking operations)]. Kyiv: NUOU. (in Ukrainian)

16. Basel Committee on Banking Supervision. The Basel Framework. 2023. URL: https://www.bis.org/baselframework/BaselFramework.pdf.

17. Natsionalnyi bank Ukrainy (2018). Polozhennia pro orhanizatsiiu systemy upravlinnia ryzykamy v bankakh Ukrainy ta bankivskykh hrupakh [Regulations on the organization of the risk management system in Ukrainian banks and banking groups]. URL:

https://zakon.rada.gov.ua/laws/show/v0064500-18# Text. (in Ukrainian)

18. Natsionalnyi bank Ukrainy (2021). Polozhennia pro zdiisnennia kontroliu za dotrymanniam bankamy vymoh zakonodavstva z pytan informatsiinoi bezpeky, kiberzakhystu ta elektronnykh dovirchykh posluh [Regulations on monitoring compliance by banks with the requirements of legislation on information security, cyber protection and electronic trust services]. URL: https://zakon.rada.gov.ua/laws/show/v0004500-21# Text. (in Ukrainian)

19. Average cost of a data breach worldwide from May 2020 to March 2023, by industry. Statista. URL: https://www.statista.com/statistics/387861/cost-data-breach-by-industry/.

20. Natsionalnyi bank Ukrainy (2017). Polozhennia pro orhanizatsiiu zakhodiv iz zabezpechennia informatsiinoi bezpeky v bankivskii systemi Ukrainy [Regulations on the organization of measures to ensure information security in the banking system of Ukraine] URL: https://zakon.rada.gov.ua/laws/show/v0095500-17# Text. (in Ukrainian)

21. Stoneburner G., Goguen A., & Feringa A. (2002) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30.

22. National Cyber Security Centre. Risk management (2023) A basic risk assessment and management method. URL: https://www.ncsc.gov.uk/collection/ risk-management/a-basic-risk-assessment-and-management-method.

23. Information Systems Audit and Control Association (2012) COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.